JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN

More Than a Feeling: Towards a Holistic Understanding of Emotions and Attitudes in Organizational Cybersecurity

Doctoral Thesis

In partial fulfillment of the requirements for the degree of

Doctor of Economics and Business Studies

(Doctor rerum politicarum, Dr. rer. pol.)

Submitted to

Justus Liebig University Giessen

Faculty of Economics and Business Studies

October 15, 2025

Author

Alexandra Freifrau von Preuschen von und zu Liebenstein

Doctoral Advisors

Prof. Dr. Monika C. Schuhmacher

Professorship for Technology, Innovation, and Start-up Management

Justus Liebig University Giessen

Prof. Dr. Verena Zimmermann

Professorship for Security, Privacy & Society

ETH Zurich

Abstract

As digital transformation accelerates, cyber threats are becoming more sophisticated and frequent, resulting in significant financial consequences. While humans have traditionally been viewed as the weakest link in cybersecurity, they are increasingly recognized as an integral part of the solution in organizational security. Emotions and attitudes significantly influence human behavior - therefore, understanding these factors in the context of cybersecurity is essential for protecting organizations.

This doctoral thesis explores emotions and attitudes in cybersecurity holistically by (1) identifying the emotions and attitudes related to organizational cybersecurity, (2) understanding the factors that contribute to emotions and attitudes in organizational cybersecurity, (3) investigating factors that can improve cybersecurity-related emotions and attitudes, and (4) applying reflections on emotions as a method to reshape how employees are viewed and how they are engaged within organizational cybersecurity contexts. To meet these goals, four studies were conducted.

In the first study, we examine the diverse range of emotions employees experience regarding organizational cybersecurity, expanding beyond the traditional focus on fear. Through a qualitative survey of 112 participants and in-depth interviews with 26 employees, we identify (partially conflicting) emotions and their causes in individual, interpersonal, and organizational factors. Our findings highlight behavioral, social, and cognitive consequences of these emotions on security perceptions and actions, leading us to propose a framework for understanding cybersecurity-related emotions and recommendations for promoting secure behavior through a human-centered approach that enhances employee well-being.

The second study explores how social and emotional dynamics affect users' engagement with security behaviors using an online survey of 496 participants. We find that social support and emotionally resonant interventions encourage greater adoption of security practices. Engagement is influenced not only by knowledge but also by emotions and social interactions, leading us to advocate for interventions that address these dimensions.

In the third study, we examine employees' attitudes toward cybersecurity through interviews and focus groups with 17 participants. The results show which components contribute to cybersecurity attitudes and which factors, particularly (social) experiences and individual factors, shape attitudes toward cybersecurity. In addition, we highlight the needs users have in order to develop positive attitudes toward cybersecurity.

The fourth study looks at how employees interact with cybersecurity in daily organi-

zational life. Through interviews with 20 participants, we identified key points of contact, such as policy awareness and training. Mapping our insights onto the NIST Cybersecurity Framework (NIST-CSF) reveals gaps in employee communication and emotional considerations. We offer recommendations for a holistic, employee-focused approach to organizational cybersecurity strategy.

Central findings of this doctoral thesis encompass (1) a framework mapping security-related emotion, their causes and consequences, (2) a framework displaying influencing factors of security attitudes alongside their components, (3) a taxonomy of factors fostering positive attitudes and positive high-arousal emotions, and (4) insights for security practitioners, management, and researchers are provided, along with a discussion of the study's limitations. The doctoral thesis concludes by suggesting research avenues, such as exploring specific stakeholders within cybersecurity, like the emotional experiences of security practitioners, to promote favorable workplace conditions and improve mental health in this domain.

Zusammenfassung

Mit der Beschleunigung der digitalen Transformation werden Cyber-Bedrohungen immer ausgefeilter und häufiger, was zu erheblichen finanziellen Konsequenzen führt. Während Menschen traditionell als schwächstes Glied in der Cybersicherheit betrachtet wurden, werden sie zunehmend als integraler Bestandteil der Lösung in der organisationalen Sicherheit anerkannt. Emotionen und Einstellungen beeinflussen das menschliche Verhalten erheblich - daher ist das Verständnis dieser Faktoren im Kontext der Cybersicherheit für den Schutz von Organisationen von entscheidender Bedeutung.

Diese Dissertation gibt Einblicke in Emotionen und Einstellungen in der Cybersicherheit indem sie: (1) die Emotionen und Einstellungen im Zusammenhang mit organisatorischer Cybersicherheit zu identifiziert, (2) Faktoren betrachtet, die zu diesen Emotionen und Einstellungen beitragen, (3) Ansätze zu untersucht, die zur Verbesserung cybersicherheitsbezogener Emotionen und Einstellungen führen, und (4) Reflektionen über Emotionen als Methode einsetzt, um die Wahrnehmung und Einbindung von Mitarbeitenden in organisationaler Cybersicherheit neu zu gestalten. Um diese Ziele zu erreichen, wurden vier Studien durchgeführt.

In der ersten Studie untersuchen wir das breite Spektrum an Emotionen, das Mitarbeitende in Bezug auf organisatorische Cybersicherheit erleben, und erweitern damit die Forschung über die bisherige Fokussierung auf Angst hinaus. Mittels einer qualitativen Befragung von 112 Teilnehmenden sowie vertiefender Interviews mit 26 Mitarbeitenden identifizieren wir (teilweise widersprüchliche) Emotionen und deren Ursachen auf individueller, zwischenmenschlicher und organisatorischer Ebene. Unsere Ergebnisse zeigen, dass diese Emotionen erhebliche Verhaltens-, Sozial- und Kognitionsfolgen für Sicherheitswahrnehmungen und -handlungen haben. Auf dieser Grundlage schlagen wir ein Framework zum Verständnis von cybersicherheitsbezogenen Gefühlen vor und geben Empfehlungen für eine menschorientierte Förderung sicheren Verhaltens, die gleichzeitig das Wohlbefinden von Mitarbeitenden steigert.

Die zweite Studie untersucht, wie soziale Faktoren (wie der Einfluss von Kolleginnen und Kollegen) sowie emotionale Erfahrungen das Engagement von Nutzerinnen und Nutzern in Bezug auf Sicherheitsverhalten beeinflussen. Anhand einer Online-Umfrage mit 496 Teilnehmenden zeigen wir, dass soziale Unterstützung und emotional ansprechende Interventionen die Bereitschaft zur Umsetzung von Sicherheitspraktiken erhöhen. Engagement wird dabei nicht nur durch Wissen, sondern auch durch Gefühle und soziale Interaktionen bes-

timmt. Daher empfehlen wir Maßnahmen, die diese Dimensionen gezielt berücksichtigen.

In der dritten Studie untersuchen wir die Einstellungen von Mitarbeitenden gegenüber der Cybersicherheit anhand von Interviews und Fokusgruppen mit 17 Teilnehmenden. Die Ergebnisse zeigen, welche Komponenten zu Einstellungen in der Cybersicherheit beitragen und welche Faktoren (insbesondere (soziale) Erfahrungen und individuelle Faktoren) Einstellungen gegenüber Cybersicherheit prägen. Zudem zeigen wir, welche Bedürfnisse Nutzende haben, um positive Einstellungen gegenüber Cybersicherheit zu entwickeln.

Die vierte Studie beleuchtet, wie Mitarbeitende im Arbeitsalltag mit Cybersicherheit umgehen. Durch Interviews mit 20 Teilnehmenden identifizieren wir Berührungspunkte wie Richtlinienbewusstsein und Schulungen. Die Abbildung unserer Erkenntnisse auf das NIST Cybersecurity Framework (NIST-CSF) offenbart Lücken in der Kommunikation mit Mitarbeitenden sowie im Umgang mit emotionalen Aspekten. Wir geben Empfehlungen für eine ganzheitliche, mitarbeiterorientierte Strategie in der organisationalen Cybersicherheit.

Zentrale Ergebnisse dieser Dissertation umfassen: (1) ein Framework zur Abbildung sicherheitsbezogener Emotionen sowie deren Ursachen und Konsequenzen, (2) ein Framework zu Einflussfaktoren von Sicherheitseinstellungen und ihren Komponenten, (3) eine Taxonomie von Faktoren, die positive Einstellungen und positive, hoch aktivierende Emotionen fördern, sowie (4) praxisrelevante Erkenntnisse für Sicherheitsverantwortliche, Management und Forschung. Darüber hinaus werden die Limitationen der Arbeit diskutiert. Abschließend werden zukünftige Forschungsrichtungen vorgeschlagen, wie die Untersuchung spezifischer Stakeholdergruppen in der Cybersicherheit, etwa der emotionalen Erfahrungen von Sicherheitsexperten, um positive Arbeitsbedingungen zu fördern und die psychische Gesundheit zu verbessern.

Acknowledgments

Before starting my PhD journey, I set out with only a handful of questions I was eager to answer; upon completing this thesis, I find myself with more questions than ever, and I am excited to see this not as an end but as the beginning of a new journey.

First and foremost, I am deeply grateful to Prof. Dr. Monika Schuhmacher for making this journey possible. Her generous support and mentoring allowed me the freedom to explore a topic that truly ignited my passion. I am especially thankful for her insightful and constructive feedback, which guided my work towards greater rigor and clarity.

I would also like to sincerely thank Prof. Dr. Verena Zimmermann, who introduced me to the field and whose role has been transformative in shaping my academic path. I am especially grateful for the opportunity to conduct a research stay at ETH Zurich under her guidance, which deeply enriched both my academic perspective and personal growth.

My heartfelt thanks go to the Usable/ Human-centered Security and Human-Computer Interaction Community for their welcoming spirit, ongoing support, and valuable feedback - yes, particularly reviewer 2! The many exchanges with researchers, some familiar from over a decade ago and others more recent, have been both enlightening and motivating.

I am especially thankful for the wonderful collaboration with Dr. Nina Gerber, who generously shared her expertise and supported my career journey. Her support has been invaluable not only to my research but also to my career development, and I deeply appreciate her encouragement and kindness throughout this journey. I would also like to thank Prof. Dr. Verena Distler and Prof. Dr. Karen Renaud for the insightful exchange and advice. Furthermore, I am sincerely grateful to Prof. Dr. Sascha Fahl for his thoughtful feedback and career support.

Special thanks to the researchers who enriched my journey with motivating discussions and shared laughter: Sara, Pascal, Neele, Lorin, Jenny, Salah, Ulli, and Nico. Furthermore, I am particularly grateful to my colleagues, past and present - Carmen, Julian, Yannick, Roman, Ricky, Vincent, Joana, Tristan, Björn, Philipp, Petrit, and Tobias - each of whom contributed to my growth, making me feel privileged to work alongside them. Working closely with Julian, Yannick, and Roman has been an enriching experience marked by excellent teamwork and a great sense of fun. I have learned so much through our work together and truly appreciated their support every step of the way.

I sincerely thank Moritz and Sabrina for their valuable insights on the practical appli-

cations of recent research and for the stimulating ideas they provided for future directions. Their support has been immensely meaningful to me.

Thank you to the student researchers Anna-Maria and Miriam for their support, as well as the students I had the privilege to supervise during their bachelor's and master's theses, particularly Carolin, Julius, and Manpreet, from whom I learned much.

I owe immense gratitude to my family and close friends. To my parents, whose unwavering belief in me showed that I can achieve anything I set my mind to; to my sister, whose constant encouragement motivated me along the way; and to Eugenie and Holger, whose thoughtful gestures of providing cake during intense writing periods brought warmth and comfort; to Elisa, for being a true source of inspiration and motivation; to Julia and Jörg, for their ongoing support; to Nanda, who reminded me of the importance of taking breaks and enjoying simple moments amid the stresses of this work.

Finally, a huge thank you to my husband, whose incredible support carried me through every high and low (and beyond fear and frustration). He stood by me during late nights, listened patiently to my countless ideas, and accompanied me through this journey with love and encouragement.

To everyone who has been part of this journey - thank you from the bottom of my heart; this thesis would not have been possible without you.

Contents

Chapter 1

Introduction

Contents

1.1 Motivation and Relevance

As digital transformation accelerates, cyber threats not only grow in sophistication and frequency but also carry severe financial implications, with the average cost of a data breach reaching $4.4 million globally and cybercrime projected to cost businesses $10.5 trillion annually by 2025 [149, 156]. Critically, cyber incidents such as ransomware attacks, data breaches, and IT outages are now perceived as the greatest risk to business worldwide, ranked #1 for the fourth consecutive year in the Allianz Risk Barometer [8].

Within this context, there is an ongoing debate about the role of humans in cybersecurity: traditionally labeled as the "weakest link," humans are increasingly recognized as integral to the solution [3, 145, 178]. Research on the latter emphasizes the importance of human involvement in securing information and systems, underscoring the need to understand human behavior to comprehend employee security practices. Commonly discussed theories for the explanation of behavior involve various factors, for instance, emotion theories that highlight the emotion-behavior relationship (e.g., [15, 97]), dual-process theories that distinguish between fast, automatic, emotion-driven responses (System 1) and slow, deliberate, analytical processing (System 2) [88] or the theory of planned behavior that involves attitudes, subjective norms and perceived behavioral control [4, 5].

In the field of cybersecurity, particularly emotions and attitudes, two closely intertwined concepts, have gained considerable attention in recent years. Previous research has demonstrated their significance across various areas, including their influence on preventive measures, compliance, and behavioral intentions [12, 21, 30, 43]. For instance, positive attitudes can foster positive cybersecurity behaviors and compliance with security policies, while negative attitudes may lead to negligence and undesirable behavioral tendencies [82, 153]. In contrast, Burns et al. [30] show that anxiety causes psychological distancing from cybersecurity, resulting in reduced preventive security measures, while interest enhances psychological capabilities, thereby increasing preventive security behavior - Happiness, however, results in psychological distancing and unfavorable security behaviors.

While existing studies on emotions and attitudes in cybersecurity show promising results, they also display heterogeneity and sometimes contradictory outcomes. Most of these studies focus predominantly on negative emotions, particularly fear, while often neglecting the complexity of emotions and attitudes involved [164].

1.2 Goals and Research Questions

In order to foster positive cybersecurity behavior in organizations, contribute to the perspective of employees as part of the solution, and, thus, improve an organization's security level, it is essential to investigate emotions and attitudes cybersecurity holistically. To address this higher-level goal, we outline four key research goals and corresponding research questions:

1.2.1 Goal 1: Identify the Emotions and Attitudes Related to Organizational Cybersecurity

Emotions. Prior research has primarily concentrated on negative emotions such as fear, sadness, and anxiety, employing quantitative methods that often use a limited range of emotion terms to capture them [1,30,32,101]. Most emotion research in the field of cybersecurity draws on concepts from related areas, such as IT usage [30], and thereby potentially misses out on emotions that might be unique to cybersecurity. Additionally, some studies encounter difficulties in accurately defining emotion terms, which hampers their ability to adequately capture these emotions [164]. However, Renaud et al. [136] provide initial findings that highlight a broader spectrum of emotions related to cybersecurity, exceeding the previous focus on negative ones. Therefore, given the emphasis on negative emotions, the diversity of results, and the frequent absence of clear definitions, it is essential to examine emotions from a holistic perspective while incorporating insights from emotion research.

Attitudes. While much research explores attitudes in cybersecurity as part of a broader investigation (e.g., [76, 143]), research that exclusively explores attitudes is limited, with only a few studies exploring this area in detail (including components of attitudes) or from a holistic perspective. Instead, some focus on related concepts such as mental models, or specific domains within cybersecurity [10, 49, 77, 136, 169].

Yet, some studies show preliminary results on the relevance of looking into components of cybersecurity. For instance, tools used to measure security attitudes often emphasize behavioral tendencies and the cognitive evaluation of these behaviors [50,52,121]. A study by de Kok et al. [39] found that employees' affective component responses to cybersecurity issues are more influential than their cognitive component when it comes to predicting behavior.

Thus, there is a lack of knowledge on the aspects of cybersecurity attitudes and a necessity of considering emotions and attitudes in cybersecurity holistically:

- RQ1a: Which emotions do employees perceive towards organizational cybersecurity?
- RQ1b: What are employees' attitudes towards organizational cybersecurity?

1.2.2 Goal 2: Understand the Factors that Contribute to Emotions and Attitudes in Organizational Cybersecurity

Emotions. Few factors have been examined in the causes of emotions related to cybersecurity. Some studies have focused on specific influences, such as how experiencing an incident can impact emotions [12]. Others have explored how induced emotions, like fear appeals, can serve as a strategy to encourage better password choices [70, 86]. However, there is still a limited understanding of the underlying causes of security-related emotions.

Attitudes. For attitudes, current research provides initial insights into the factors influencing cybersecurity attitudes. For instance, technological factors such as software updates [49], individual factors such as knowledge and expertise [121, 142], or social and organizational

factors such as norms [143]. There is only a limited understanding on influencing factors to the concept of attitudes in organizational security.

Consequently, there is a research gap on factors that contribute to emotions and attitudes in organizational cybersecurity.

- RQ2a: What causes emotions in the context of organizational cybersecurity?
- RQ2b: Which factors influence employees' attitudes towards organizational cybersecurity?

1.2.3 Goal 3: Investigate Factors to Improve Cybersecurity-related Emotions and Attitudes

Emotions. While many articles in prior research focused on enhancing the usability of security [99], few articles have examined how to improve emotional and attitudinal engagement with cybersecurity. While there is research on behavioral consequences, the number of emotions explored is mostly limited to negative emotions. Further, only a few articles provide insights beyond behavior, and for instance, Dupuis et al. [43] demonstrate that there might be short-term positive behavioral consequences of fear appeals - these, however, are accompanied by negative affect and potential unfavorable long-term consequences. Other articles show additional psychological outcomes, such as burnout and fatigue [35, 125]. As research on the outcome of emotions in cybersecurity is limited and mostly restricted to behavioral consequences, there is a need to examine the consequences of specific emotions beyond behavior to understand which ones are valuable for improvement. Following the results from RQ3a, we investigate a positive high-arousal emotion in RQ3b.

Attitudes. Organizations already employ various strategies to promote positive cybersecurity attitudes that encourage secure behaviors. The three most common approaches are (1) modifying cognitive attitudes by using fear appeals to emphasize the potential consequences of non-compliance [24, 43, 86, 132], (2) fostering positive affective attitudes making cybersecurity "fun" [20, 151], or (3) no attitude appeal, implementing a more traditional approach that focuses on the transfer of factual knowledge [43]. Although these methods are widely used, not many exceed these practices. Exploring the factors that foster positive attitudes is essential for enhancing cybersecurity behavior.

Thus, we formulate the following research questions:

- RQ3a: What are the consequences of emotions in organizational cybersecurity?
- RQ3b: How can cybersecurity be made more enjoyable?
- RQ3c: What are the needs for positive cybersecurity attitudes (and, ultimately, positive cybersecurity behavior)?

1.2.4 Goal 4: Apply Reflections on Emotions as a Method to Reshape how Employees are Viewed and Engaged Within Organizational Cybersecurity Contexts

The goal of adopting a human-centered approach to change employees' perspectives has been a long-standing effort [3, 178]; however, organizations still struggle to encourage positive cybersecurity behaviors among their staff [13, 179]. This challenge may stem from a lack of integration of employees' perspectives into the organization's cybersecurity practices [178]. In our research (refer to Paper A in 1.3), we found that emotions can serve as a valuable tool for gaining insights into not only cybersecurity-related feelings but also the underlying emotional experiences, their causes, and consequences. Therefore, in a follow-up study, we aim to enhance employees' integration into cybersecurity frameworks by utilizing reflections on emotions to identify key points of contact between employees and cybersecurity and ultimately identify gaps in a selected cybersecurity framework regarding employee aspects.

- RQ4: Can reflections on emotions be used as a way to improve current views on employees in organizational cybersecurity?

1.3 Outline and Publications

To achieve the research goals outlined in Section 1.2, we undertook four research projects. Two papers focused on emotions, a third paper examined attitudes, and a fourth one used emotions as a tool to enhance employees' integration into organizational cybersecurity (see Figure 1.1 for the mapping between goals and papers and Figure 1.2 for the thesis overview):

Paper A: Exploration of Emotions towards Organizational Cybersecurity

Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. 2024. Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity. In Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). USENIX Association, Philadelphia, PA, 623–642. https://www.usenix.org/conference/soups2024/presentation/von-preuschen
Rating: CORE: B
Awarded Distinguished Paper

Summary: We investigated the wide spectrum of emotions employees experience in organizational cybersecurity, moving beyond the traditional focus on fear and negative affect. Using a qualitative survey (N=112) and in-depth interviews (N=26), the study identified diverse and sometimes conflicting emotions, classified through the circumplex model of affect. We found causes rooted in individual, interpersonal, and organizational factors. Our research

highlights that these emotions have significant behavioral, cognitive, and social consequences, including impacts on security perceptions, actions, and even broader work experiences. We propose a framework to map the complexity and spill-over effects of cybersecurity-related emotions and make recommendations for fostering secure behavior using a human-centered approach that mitigates negative effects while promoting user well-being.

Paper B: Improving Emotions Towards Cybersecurity

Nina Gerber, Verena Zimmermann, Alexandra von Preuschen, and Karen Renaud. 2025. Unpacking the social and emotional dimensions of security and privacy user engagement. In Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025). USENIX Association, Seattle. 535-554. https://www.usenix.org/conference/soups2025/presentation/gerber
Rating: CORE: B

Summary: We examined how social factors (such as peer influence and normalization of discussions) and emotional experiences shape users' engagement with security and privacy (S&P) behaviors using an online survey with a larger sample size (n = 496). We reveal that fostering social support and emotionally resonant interventions can drive greater user adoption of positive S&P behaviors. Our findings underscore that S&P engagement is influenced not only by knowledge or awareness but also by the feelings of users and the quality of social interactions surrounding these topics. We advocate for designing interventions that recognize and leverage these social and emotional dimensions.

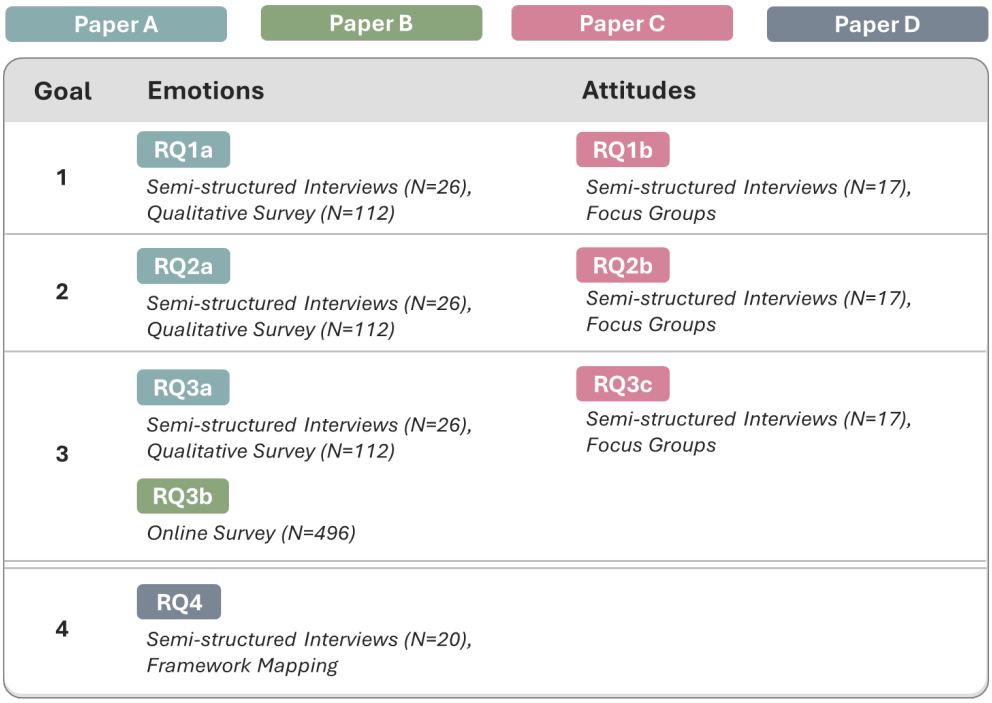


Figure 1.1: Outline of the publications included in the doctoral thesis.

Paper C: Exploration and Improvement of Attitudes Towards Organizational Cybersecurity

Alexandra von Preuschen, Carolin Benda, Monika C. Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3706598.3713538
Rating: CORE: A*, VHB: A

Summary: We holistically explored employees' attitudes towards cybersecurity using semi-structured interviews and focus groups (N=17), uncovering the wide-ranging factors that influence these attitudes and the needs employees have for fostering more positive ones. The study challenges the notion of employees as "weakest links", instead highlighting their potential as key defenders when their attitudes are better understood and addressed. We identified that factors such as direct and indirect personal experiences and individual factors shape cybersecurity attitudes and engagement. The findings emphasize that supporting employee needs and leveraging appropriate emotional drivers can promote positive cybersecurity behaviors in organizations.

Paper D: Emotions as a Method to Extend Cybersecurity Frameworks with a Human-centered Lens

Alexandra von Preuschen, Roman Henke, Manpreet Kaur, Julian Nickel, and Monika C. Schuhmacher. 2025, in press. Towards an Employee-Centric Framework of Cybersecurity. In European Symposium on Usable Security (EuroUSEC 2025), Manchester, UK.
Rating: CORE: Unrated.

Summary: We explored how employees experience and engage with cybersecurity in daily organizational life, moving beyond traditional frameworks' technical and compliance-focused perspectives. Using semi-structured interviews (N=20), we identified key points of contact, such as policy awareness, technical controls, incident response, training, and communication, between employees and security. We highlight the important influence of emotions, usability, and social dynamics on security behaviors. By mapping these insights onto the NIST Cybersecurity Framework (NIST-CSF), we revealed gaps such as insufficient attention to employee communication, emotional impacts, and role clarity. We propose recommendations for practitioners, such as addressing usability and engagement in security measures, improving visibility and accessibility of support, and acknowledging emotional and psychological impacts. We emphasize the need for a holistic, employee-focused approach to organizational cybersecurity.

Further Publications (Not Included in This Thesis). In addition to the publications that form the main body of this work, I collaborated on other peer-reviewed articles during my time as a PhD student, which played a significant role in establishing the foundation of this thesis.

- Alexandra von Preuschen, Verena Zimmermann, and Monika C. Schuhmacher. 2023. How do you Feel about Cybersecurity? – A Literature Review on Emotions in Cybersecurity. In International Symposium on Technikpsychologie (TecPsy 2023) Sciendo. 1-13.

- Alexandra von Preuschen, Yannick N. Amend, Roman Henke, Luca Wrede, Monika C. Schuhmacher, and Verena Zimmermann. 2025. Climbing towers or looking at flowers: Exploring Young Adults' Needs for Effective Cybersecurity Education Through Design Thinking and LEGO Serious Play. In Mensch und Computer 2025 - Workshopband. Gesellschaft für Informatik e.V.. MCI-WS05: 11th Workshop on Usable Security and Privacy. Chemnitz. 31. August - 03. September 2025. DOI: 10.18420/muc2025-mci-ws05-351

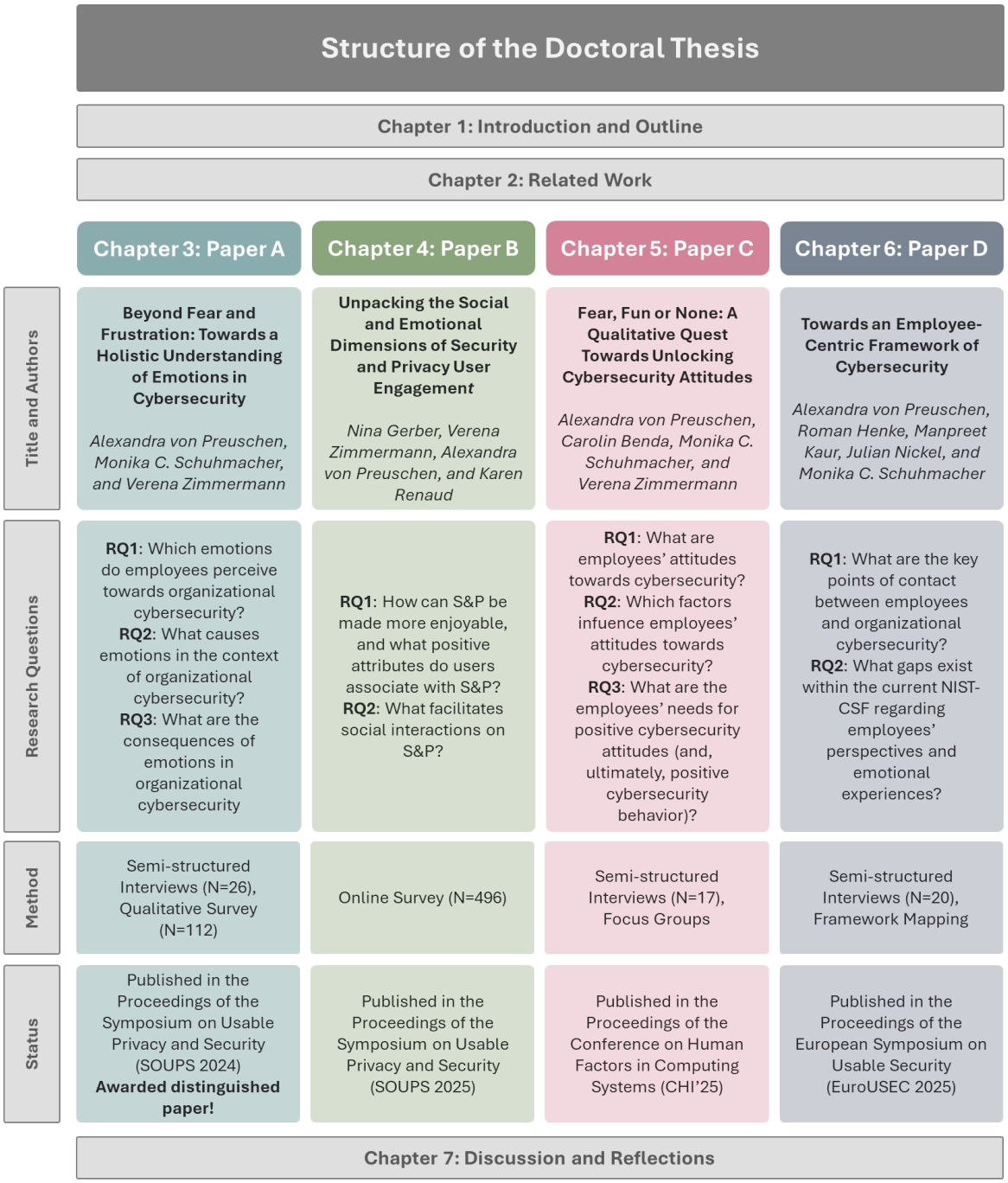


Figure 1.2: Structure of the doctoral thesis. The research questions shown in this figure refer to the actual research questions within the papers. Please note that the research questions in Paper B extend beyond the scope of this doctoral thesis and are only partially addressed in the discussion and reflection sections.

Chapter 2

Related Work

Contents

2.1 Employee's Role in Organizational Cybersecurity

2.1.1 Human-centered Cybersecurity

For decades, there has been an ongoing debate regarding the role of humans in cybersecurity. On one hand, humans have often been considered the weakest link or "problem" in cybersecurity [145]. Here, focus is placed on bringing users to comply with often strict and complicated security policies and requirements (e.g., [29, 111]). On the other hand, another line of research argues that users should not be viewed as enemies but instead as part of the solution [3, 178]. This perspective emphasizes the integration of human factors in security design, the need for security measures to be both usable and cognitively manageable for individuals [135, 144]. For example, in the context of password management, it recognizes the limitations of human cognitive capabilities when it comes to remembering multiple complex and lengthy passwords. A password manager provider reports that, on average, in 2024, users have 255 passwords for both personal and work-related accounts [118] - Expecting users to manage such a wide array of passwords, along with their corresponding usernames, may be overly demanding. Therefore, a human-centered security approach advocates for designing security measures that align with human nature and capabilities. It generally highlights the crucial role of end-users in securing information and systems, and emphasizes the social, organizational, and technological factors that influence people's understanding of and interactions with cybersecurity [117, 133]. The research field explores topics such as user motivation, security communication, or participatory design [133]. In contrast, the field of usable security, originally foregrounded by Whitten and Tygar's [172] landmark study "Why Johnny Can't Encrypt", focuses on designing security mechanisms and user interfaces that people can use effectively, efficiently, and with satisfaction, without undermining security objectives. While the definition of usable security in a narrow sense only covers parts of the field of human-centered security, the terms of both concepts are often used interchangeably.

While human-centered security explores various contexts, such as private (e.g., [52, 64]) and workplace environments (e.g., [31, 79]), this dissertation will exclusively focus on the latter.

2.1.2 Human Aspects in Cybersecurity Frameworks

Cybersecurity frameworks, such as ISO/IEC 27001 and COBIT, are structured sets of guidelines, best practices, and standards designed to help organizations define cybersecurity strategy and manage cybersecurity risks in a systematic and comprehensive manner [11, 114, 158]. One of the most widely recognized frameworks in cybersecurity is the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST-CSF) [114, 116], which is structured around six core functions: Identify, Protect, Detect, Respond, Recover, and Govern (the latter added in version 2.0). These functions help organizations identify their assets and risks, ensuring their protection, detecting incidents,

responding to breaches, and restoring normal operations. Each function includes categories and subcategories that address technical, administrative, and governance aspects [114, 116].

The framework remains heavily focused on technical controls and compliance, with human aspects featured primarily in operational subcategories like training, access management, and incident response [115]. Employees are often conceptualized as passive recipients expected to follow procedures, with limited recognition of the broader psychological, social, and emotional factors that have been highlighted in research to influence secure behavior [51, 164]. Even though Rohan et al. [137] mapped human factors to the NIST-CSF and found behavioral elements in some functions, their top-down analysis shows that key functions, such as Identify and Recover, still largely neglect employee engagement and experience. As a result, the human factor is often constrained within technical categories, rather than being addressed holistically as an integral, dynamic part of organizational cybersecurity.

2.2 Emotions

2.2.1 The Concept of Emotions

Definition of Emotions and Delimitation of Related Concepts. The concept of emotions is frequently oversimplified in cybersecurity. Terms such as affect, mood, feelings, and emotions are often used interchangeably, creating conceptual confusion that undermines our understanding of these distinct psychological phenomena [47, 58, 148].

Affect serves as an umbrella term encompassing both moods and emotions, characterized by valence (positive or negative) and varying degrees of arousal [33, 63, 140]. More precisely, affect represents the pre-subjective and non-conscious encounter with continuously varying intensities, describing the body's readiness for interaction [109]. *Feelings* are mental sensations that include experiences like coldness and that are reviewed against past experiences [106,150]. *Emotions* express these feelings in social contexts, turning internal sensations into experiences that can be communicated to others [46,150]. They are typically short-lived and intense, and they can appear as either dispositional tendencies (trait-like characteristics) or temporary states that are experienced over brief periods [83]. In contrast, *mood* represents prolonged, generalized emotional states that persist for hours or days without direct relation to specific events [83]. Emotions, unlike moods or the broader concept of affect, possess a high degree of informative content for the individual and significantly shape perception, decision-making, and behavior [108].

Emotion Theories. Emotion theories provide foundational perspectives on how emotions arise and their functional significance. Gross and Feldman-Barrett describe a continuum of perspectives on emotion, varying in their core assumptions concerning emotions [68]. According to this approach, *basic emotion models* view emotions as a limited number of biologically basic states that are unique from other states, such as cognition, and are caused by a dedicated mechanism (e.g., [46, 84, 100]). For instance, fear as a result of an immediate

threat or danger. *Appraisal Models*, in contrast, view emotions as resulting from specific cognitive factors that help individuals make sense of the world. These models emphasize the importance of cognitive evaluation, as noted by researchers such as Roseman (1991), Lazarus (1991), and Frijda (1988) [57, 97, 138]. According to Lazarus (1984), the individual interprets a stressor (primary appraisal) and analyzes their available resources (secondary appraisal) to form a coping response and, thus, behavioral responses [98]. For instance, fear of public speaking arises when a person appraises the situation as threatening, for example, fearing negative judgment from the audience. If they see it as a challenge instead, fear may not occur. While appraisal theories perceive emotions as responses to triggers or cognitive evaluations, which lead to universal behavioral strategies [47, 59], theories of constructed emotions highlight the diversity in emotional experiences and the actions that follow [18]. Here, emotions are not seen as universal, biologically wired reactions to stimuli; rather, they are actively shaped by the brain based on prior experiences, contextual factors, and sensory information [53]. Thus, emotions result from a process that categorizes sensations by utilizing past experiences - They create situational conceptualizations that align with current circumstances and bodily needs, ultimately guiding actions [16, 19].

Measurement. Measuring emotions presents significant challenges due to their multidimensional nature. Common measurement approaches are accompanied by advantages and disadvantages. Quantitative methods like word counts and facial recognition are popular but limited because people express emotions differently, more complex emotions may be missed, and facial cues can be misinterpreted or mimicked [57, 80, 107, 155]. Other measurement domains that offer a rather observer-independent, standardized tool are the analysis of facial muscle activity, vocal acoustics, or autonomic nervous system activity [128]. Objective measures in the brain and body are often weakly correlated and do not reliably distinguish between emotions like anger, sadness, and fear [15, 103, 104]. In contrast, subjective experiences can be captured using the affect grid [140], or the Positive Affect and Negative Affect Scale [170]. Subjective approaches carry certain risks. For instance, during an interview, the interviewee needs to rely on their past emotional experiences while also possessing the ability to reflect on and articulate these experiences. Additionally, they must be able to manage any fears related to social desirability [128]. A multimodal approach that incorporates multiple measurement domains is recommended, alongside tailoring the measurement strategy to the emotion theory that underpins the research project [18, 128].

2.2.2 Emotions in Cybersecurity

In a systematic literature review, we examined the role of emotions in current cybersecurity literature [164]. To capture the interdisciplinary essence of the topic, data from various databases and a range of search terms were used to encompass multiple definitions. Papers that only incidentally touched upon emotions (e.g., as casual remarks in interviews without

elaboration), treated emotions solely as traits within the realm of personality, focused on related constructs like stress, or failed to provide a clear distinction between stress and emotions were excluded from the analysis, resulting in a final analysis of 24 papers.

Cybersecurity-related Emotion Identification and Measurement. Literature was then classified into three fundamental streams: studies exploring (1) the existence of affect or emotions (e.g., [27, 34, 161]), (2) investigating explicit emotions (e.g., [30, 32]), or (3) elucidating complex constructs (e.g., [35, 125]). In category 2, a clear trend towards negatively-valenced emotions was observable (fear (e.g., [1, 32]), anxiety (e.g., [12, 30])). Concerning the measurement of emotions, a variety of approaches were observed, both in terms of operationalization and measurability. For instance, within the first category, exploring the existence or impact of affect, a diversity of methodologies was employed (e.g., interview data [21], a combination of EEG and behavioral data [34] or questionnaire data [39]). In contrast, the measurement of emotions primarily relied on emotion lists, from which participants were to select the relevant emotions (e.g., [27, 48]). Only two studies pursued a qualitative-exploratory approach (e.g., [28, 136]). In most other cases, including the second category, the studied emotions were derived from research or theories of related disciplines (e.g., emotions related to IT usage, e.g., [30]).

Focus of Cybersecurity-related Emotions. It is noteworthy that the examined studies exhibited various focuses, distinguishing between a focus on emotions and a focus on cybersecurity. In terms of emotions, a distinction was made between incidental emotions (regardless of the given decision/perception, e.g., anger over a decision by a superior affecting susceptibility to phishing emails) and integral emotions (relevant to the given decision/perception, e.g., fear of phishing emails affecting susceptibility to phishing emails). Integral emotions were directed toward a specific object (e.g., [30, 39, 48]), the global cybersecurity concept (e.g., [136]), oneself (e.g., [27, 134]), or others (e.g., [12, 27]). Additionally, a distinction was made between induced and existing emotions, with induced emotions, such as fear appeals, being particularly prevalent (e.g., with the aim of motivating the choice of a strong password; [43, 86]).

Regarding the focus on cybersecurity, we differentiated three process phases and an umbrella term. The process phases represent specific subareas of cybersecurity. 'Pre-incident' (a) deals with actions, including education, to prevent an incident, 'incident' (b) involves detecting an attack and taking action to bring it under control, and 'post-incident' (c) involves actions to minimize the impact of an incident, restore or modify the normal state, and the general handling of an incident within a company. The category 'global' (d) describes subareas that exist across all process phases (e.g., the relationship between lay users and experts, emotions toward the entire concept of "cybersecurity").

Effects of Cybersecurity-related Emotion. Irrespective of the measurement methodology, focus, or phase, we identified emotions and affect as central drivers of behavior within cybersecurity. In the (a) pre-incident stage, positive emotions, particularly interest, posi-

tively influence preventive behaviors, while negative emotions lead to undesirable behaviors such as avoidance [21, 30]. Induced negative emotions, in contrast, such as fear appeals in awareness campaigns, can be effective, if additional variables (such as strengthening of self-efficacy) are minded. However, despite the eventual positive direct effect, they can trigger emotions like sadness, which may result in avoidance, and emotional overload can lead to fear fatigue [41, 132, 176]. (b) During incidents, emotions play a crucial role in susceptibility, with fear and anxiety influencing responses to phishing attacks [1]. Also, incidents can result in a broad variety of emotions, which determine behavioral tendencies and coping strategies [12, 28]. (c) Post-incident, outward emotion-focused coping positively affects security behavior, while inward-looking processing leads to denial. Employer responses influence employee emotions, with shame leading to negative actions and guilt fostering self-acceptance and learning [101, 134]. Globally, negative emotions, in particular fear and anxiety, dominate in cybersecurity contexts, affecting not only behavior but also well-being and job satisfaction [32, 110, 136]. This emotional spillover contributes to phenomena like cybersecurity fatigue and burnout [35, 125].

Challenges to Emotion Research in Cybersecurity. Based on the review, five interconnected challenges in researching emotions in cybersecurity are derived:

- First, the *conceptualization of emotions and cybersecurity* introduces risks due to the interchangeable use of terms like "affect," "mood," and "emotions" without considering their nuanced differences [108]. Defining emotions solely by valence proves insufficient in cybersecurity, where fear and anxiety, though sharing valence, lead to distinct behaviors [12, 59, 139].

- Second, *measuring emotions* confronts difficulties due to their multidimensional nature, with quantitative methods struggling to capture complexity and potential biases [107, 155]

- Third, *measuring cybersecurity* behavior via surveys risks oversimplification and may miss nuanced behaviors, particularly in the presence of strong negative affect [21, 92]

- Fourth, *delimiting the context of emotion research* is crucial, as perceptions differ in private and professional settings, and the definition of security varies across companies [66, 134]

- Finally, the *complexity of emotions and cybersecurity* poses challenges, with contradictory emotions, varying emotions associated with different aspects within cybersecurity, and potential spill-over effects on associated aspects of work and life [41, 54, 136]

2.3 Attitudes

2.3.1 The Concept of Attitudes

Definitions of Attitudes. Allport [9] describes attitudes as a psychological and neurological state of preparedness, shaped by experience, which influences an individual's responses to related objects and situations. In contrast, Eagly and Chaiken (1993) define attitudes as a psychological tendency that reflects the evaluation of a specific entity, which can vary in degrees of like or dislike [44]. Similarly, Ajzen characterizes attitudes as an individual's tendency to react positively or negatively towards an object, person, institution, event, or any other distinguishable element of their environment [4, 5]. In this approach, it is assumed that the underlying attitude affects behavioral intention, which in turn directly influences the actual behavior. [5].

The tripartite model of attitude extends previous approaches by proposing a structure that includes affective, cognitive, and conative components, allowing for potentially conflicting elements [6, 7, 175]:

1. **Affective component**

   Definition: The affective component refers to the emotional responses that individuals have towards objects of their attitudes [2, 157].

   Example: An example of the affective component is the fear of making mistakes when implementing a new cybersecurity measure.

2. **Cognitive component**

   Definition: The cognitive component of attitude involves the beliefs and thoughts an individual holds about an attitude object [2, 157].

   Example: Beliefs that cybersecurity training cannot prevent social engineering attacks represent a negative cognitive component of attitude.

3. **Conative component**

   Definition: The conative component of attitude concerns behavioral inclinations, intentions, commitments, or actions in respect of an object, event, or institution. Behavioral attitudes can be investigated by considering what individuals say, plan to, or would do with regard to the attitude object [7].

   Example: Choosing not to participate in additional cybersecurity training may reflect a negative conative component.

Delimitation of Related Concepts. While related concepts are closely linked to attitudes, it is important to distinguish between them. For instance, emotions (see 2.2 for further information) differ from the affective component of attitudes in that they tend

to be unstable, lack an evaluative predisposition, and are generally intense but short-lived [2, 83, 157]. In terms of the cognitive component, the idea of belief is closely associated with this concept. A set of beliefs is sometimes referred to as a mental model [119]. However, mental models are better described as dynamic, systemic representations of reality [85]. This flexibility sets them apart from the relatively stable, evaluative judgments about specific objects that are part of the cognitive component of attitudes [5, 105]. Further, the conative component of attitudes needs to be delimited from behavior itself. This component does not directly predict specific behavioral outcomes but rather signifies a predisposition toward certain actions [175] based on observed prior actions and verbal statements about future intentions [25]. Rather than seeing affect and cognition as direct predictors of behavior, the model integrates three interacting components at one level [4].

Attitude Formation. Attitude formation is influenced by a combination of psychological, social, and cognitive factors. For instance, social learning theory posits that attitudes develop through observation, reinforcement, and interaction with the surrounding environment [14]. Evaluative conditioning and related learning approaches emphasize that attitudes can emerge from stimulus pairing and associative learning [166,167,171]. Other theories zoom into attitude change. For instance, the Elaboration Likelihood Model explains how persuasive messages can lead to attitude change through either central or peripheral processing routes [123]. The Knowledge-Attitude-Behavior model, views knowledge independent of the communication channel as an anticipant of attitudes [121]. Other theories focus on the fundamental human drive for psychological consistency. Festinger's cognitive dissonance theory explains how attitudes change when individuals experience psychological discomfort from holding conflicting beliefs or when their actions contradict their attitudes [54]. Similarly, balance theory, proposed by Heider [73, 74], suggests that individuals strive for consistency in their relationships and attitudes, seeking to maintain balanced cognitive structures by altering attitudes when inconsistencies arise.

Attitude-Behavior Relationship. While attitudes are recognized as a key factor in explaining behavior, actions are more accurately understood as resulting from an interaction between attitudes and various influences - such as environmental factors, situational contexts, and individual differences. For instance, the theory of planned behavior outlines behavior as a result of the interaction between subjective norms, attitudes, and perceived behavioral controls [7] or the theory of reasoned action integrating attitude and subjective norms [56]. The Knowledge-Attitude-Behavior Model, in contrast, displays a direct connection of attitude and behavior [121]. The tripartite model of attitudes does not conflict with these theories, despite incorporating a behavioral component.

Measurement. There are generally (1) direct, (2) indirect measurement approaches, as well as (3) behavioral and observational methods for measuring attitudes [94]. The most common approaches are self-report scales, such as the Likert scale (which asks respondents to rate agreement with statements) [102] or the semantic differential scale (where respon-

dents rate a concept using bipolar adjectives, e.g., good-bad) [120] and interviews (that can vary in their level of standardization [75]). While direct measures are efficient and provide in-depth understanding, they can be affected by social desirability bias and intentional response editing. In contrast, implicit measures like the Implicit Association Test [67] and behavioral observations (such as non-verbal or linguistic behavior) [94] are used to uncover unconscious or automatic attitudes. Unconscious attitude measures may be less influenced by self-presentation. However, their interpretation can be less straightforward and may not consistently align with detailed self-reports.

2.3.2 Attitudes in Cybersecurity

Impact of Cybersecurity Attitudes. Attitudes towards cybersecurity have been increasingly recognized as a critical factor influencing cybersecurity behavior. Researchers have observed positive effects of attitudes towards the intention of using anti-spyware or overall compliance [29, 40, 81]. Similarly, Hu et al. [81] identified a positive relationship between attitudes and compliance with security policies, while Bulgurcu et al. [29] emphasized the impact of attitudes on employees' compliance to these policies. Awareness of information security positively influences attitudes, while the interference of security measures with daily tasks tends to foster negative attitudes [76]. Concepts related to attitudes, like cybersecurity fatigue highlighted by Reeves et al. [131], demonstrate how feeling overwhelmed can lead to disengagement and noncompliance without malicious intent [35]. In general, prominent theories in cybersecurity research, like the theory of planned behavior and the knowledge-attitude-behavior model, emphasize attitudes as a key factor in predicting cybersecurity intentions and behaviors [29, 71, 81, 121, 143]. Generally, various contexts have been observed, such as user data sharing across online services and companies [22] or consumer attitudes toward privacy and security in adopting Internet of Things devices, fitness trackers, and mental health applications [60, 62, 91, 96]. Regarding how various components of attitudes affect behavior, de Kok et al. [39] showed that both the affective and cognitive components enhance the intention to engage in cybersecure practices, with the affective component exerting a more significant influence than the cognitive one. Similar concepts to attitudes have also shown significant influence on cybersecurity behavior. For example, Reeves et al. [131] highlight that employees may find cybersecurity actions overwhelming, resulting in disengagement - a phenomenon known as cybersecurity fatigue. This state, characterized by feeling tired from security requirements, can lead to noncompliance without malicious intent [35].

Components of Cybersecurity Attitudes Research on cybersecurity attitudes remains limited in scope and depth. Some studies focus on related constructs such as emotions, mental models, or specific cybersecurity domains [10, 49, 77, 136, 169].

For example, research on mental models displays that users with lower expertise believe that attackers primarily target large institutions [169]. Moreover, cybersecurity is frequently perceived as mystical or unknown [36] or associated with fear and complexity rather than positive attributes despite recognition of importance, underscoring the affective and cognitive components [136]. Exceeding the concept of cybersecurity, aspects of cybersecurity such as encryption for personal communication are sometimes also negatively associated with suspicion [173].

Measurement tools predominantly target cognitive and conative dimensions. Instruments such as the SA-6, Security Behavior Intentions Scale (SeBIS), and Human Aspects of Information Security Questionnaire (HAIS-Q) focus similarly on behavioral tendencies and cognitive evaluations [50, 52, 121].

Impacting Factors on Cybersecurity Attitudes. Current research gives a first understanding of the factors that impact cybersecurity attitudes: For instance, *Technical Factors.* Fagan et al. [49] demonstrated that software update prompts can evoke negative feelings and foster negative beliefs about the updates. Similarly, Herath and Rao [76] found that when security measures interrupt routine tasks, negative attitudes can arise. Additionally, Arnold et al. [10] found that introducing multi-factor authentication can lead to negative emotions without necessarily improving the perception of security.

Further, *Individual Factors.* Knowledge and expertise play substantial roles in shaping cybersecurity attitudes [121, 142]. Particularly, experts display more complex mental models than novices in the prevention of phishing attacks [177]. Concerns about security breaches and perceived response costs further mediate these attitudes [76, 143].

Lastly, *Social and Organizational Factors.* Research indicates that social factors, such as norms and collaboration, significantly influence cybersecurity attitudes [143]. Studies highlight that community involvement and experiences shape individual perceptions [87, 143, 162]. Menges et al. found that communication between employees and IT staff affects security attitudes, highlighting the significance of interpersonal relationships [110].

Chapter 3

Paper A: Exploration of Emotions Towards Organizational Cybersecurity

The paper was published as follows:

Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. 2024. Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity. In Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). USENIX Association, Philadelphia, PA, 623–642. https://www.usenix.org/conference/soups2024/presentation/von-preuschen

Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity

Alexandra von Preuschen
Justus-Liebig-University Gießen

Monika C. Schuhmacher
Justus-Liebig-University Gießen

Verena Zimmermann
ETH Zurich

Abstract

Employees play a pivotal role for organizational cybersecurity, making understanding the human factor in the context of cybersecurity a critical necessity. While much is known about cognitive factors, less is known about the role of emotions. Through a qualitative survey (N = 112) and in-depth interviews (N = 26), we holistically investigate the causes, types and consequences of emotions in the context of cybersecurity. We demonstrate the existence of diverse, even conflicting emotions at the same time and classify these emotions based on the circumplex model of affect. Furthermore, our findings reveal that essential causes for cybersecurity-related emotions include individual, interpersonal and organizational factors. We also discover various cybersecurity-relevant consequences across behavioral, cognitive and social dimensions. Based on our findings, we provide a framework that unravels the complexity, impact and spill-over effects of cybersecurity-related emotions. Finally, we provide recommendations for promoting secure behavior with a human-centered lens, mitigating negative tendencies, and safeguarding users from unfavorable spill-over effects.

1 Introduction

For decades, the human factor has been considered the weakest link in organizational cybersecurity, often dismissed as lazy or demotivated [23, 84]. This perception has frequently resulted in cumbersome security processes or the use of fear appeals to enforce security guidelines [7, 35, 90]. These everyday experiences with cybersecurity likely cause a spectrum of emotions associated with the term which, in turn, might impact cybersecurity behavior.

As our acknowledgment of humans as integral components of organizational socio-technical systems deepens, there is an increasing importance in understanding human interaction with cybersecurity [17, 54, 76, 83, 90]. In organizational contexts, understanding employee contributions to cybersecurity and the related role of emotions is crucial to protect both companies and the well-being of the employees themselves. Insights from studies exploring the broader impact of emotions in areas such as decision-making, memory and learning, attitude change, or workplace dynamics in general [4, 50, 51, 69, 70], demonstrate the significant and far-reaching impact of emotions in shaping individual actions and cognition towards an object [41, 49].

In the field of cybersecurity, preliminary research also indicates a significant impact of emotions on preventive measures, compliance, and behavioral intentions [6, 16, 22, 35]. Notably, a study by Burns et al. [22] demonstrates that anxiety prompts psychological distancing from cybersecurity, resulting in decreased preventive security measures, while interest leads to the expansion of psychological capabilities, thereby increasing the manifestation of preventive security behavior. Consequently, acknowledging and comprehending cybersecurity experiences and their resulting emotions as well as their consequences is a crucial necessity.

Despite these insights, existing studies related to emotions in cybersecurity exhibit heterogeneity, sometimes contradictory results, mainly focus on negative emotions, particularly fear, and often neglect the complexity of emotions occurring [88]. Consequently, a notable gap persists in the comprehensive understanding of emotions in the context of cybersecurity, including their causes and consequences.

Against this background, this research seeks to close the existing gap by exploring the role of emotions in the context of organizational cybersecurity. To that end, we captured first-hand emotional experiences of employees including experts' as well as employee perspective through a qualitative survey (n = 112) and in-depth interviews (n = 26) that can account for the complexity of emotions. For a holistic understanding, we applied a multi-method approach in the interviews exploring emotions related to cybersecurity in general and specific cybersecurity areas in a multi-faceted way: a) verbally, b) through a non-verbal Product Emotion Measurement Instrument (PrEmo [33, 34]), c) through emotion-related word lists, and d) ratings of emotion intensity. Further, to navigate the complexity of emotions, we applied the circumplex model of

affect [73]. Additionally, emotion causes and consequences were explored. As we know little on how emotions are caused, which emotions occur and what consequences result from them in the context of cybersecurity behavior, we adopt an exploratory and phenomenological qualitative approach. This methodological choice allowed for addressing the complexity of the research topic, while opening the problem space to empathize with employees and to identify emerging patterns [67]. Overall, we investigate three research questions (RQs):
RQ1: Which emotions do employees perceive towards organizational cybersecurity?
RQ2: What causes emotions in the context of organizational cybersecurity?
RQ3: What are the consequences of emotions in organizational cybersecurity?
Our findings show that emotions are caused by four essential themes: individual perceptions, cybersecurity perceptions, interpersonal factors, and organizational factors. Further, we identified multiple emotions towards cybersecurity, extending prior literature. Participants not only but predominantly expressed negatively valenced emotions and overall low-arousal emotions (e.g., 'fearful') were more common than high-arousal ones (e.g., 'interested'). Finally, we find various impacts of cybersecurity-related emotions on individual's cybersecurity perceptions and behaviors, that even extend to other areas of life.

The contribution of our research is three-fold: 1.) We offer a holistic and in-depth exploration of the role of emotions in cybersecurity by employing a multi-modal approach; 2.) Our study develops a theoretical model in the analysis of causes, consequences, and emotions classifying a wide spectrum of cybersecurity-related emotions; and 3.) We provide recommendations for practitioners to enhance favorable consequences, mitigate unfavorable ones among employees, and maintain employees' mental health.

2 Related Work

The following section introduces the concept of emotions and the current state of emotion research within cybersecurity.

2.1 The concept of emotions

Despite the common misconception that emotions are subjective and unpredictable, research demonstrates that affective reactions are often more similar across individuals than cognitive evaluations [72]. Nevertheless, the oversimplification of the concept of 'affect', 'mood' and 'emotion' is a common challenge, often resulting in the terms being used interchangeably [15, 38, 82] with 'affect' often serving as an umbrella term for 'mood' and 'emotion' [28, 73]. 'Mood' is unrelated to specific objects, yet, can result from an emotion when maintained over a longer time [41, 49]. In contrast, emotions, such as happiness or anger, describe an individual's mental state based on a reaction to a person, event, or object, preparing for action and serving a social function [41]. Feelings, unlike emotions, are purely mental and involve sensations like touch, which are compared to past experiences [60, 86]. Emotions, in turn, express these feelings and are eventually placed in a social context [37, 86]. According to the theory of constructed emotions, emotions are not pre-wired, universal responses to stimuli. Instead, they are actively constructed by the brain based on past experiences, contextual cues, and sensory input [11]. While some theories view emotions as responses to triggers or cognitive evaluations, leading to universal behavioral strategies (e.g., fear triggering a specific facial expression followed by flight behavior [38, 42]), the theory of constructed emotions emphasizes the diversity in emotional experiences and their subsequent actions [12]. Here, emotions describe the result of a process that categorizes sensations by drawing on past experiences and creating situational conceptualizations that best fit the current situation and bodily needs to ultimately guide action [10, 13]. Thus, there is the option to induce emotion consciously, for example by the use of fear appeals to modify behavioral tendencies [58].

Various frameworks for classifying emotions exist such as the circumplex model of affect that offers a structured classification of emotions based on two key dimensions: The vertical axis 'valence' refers to a stimulus's pleasantness ranging from negative to positive; the horizontal axis 'arousal' describes a stimulus' intensity, or the degree of activation of the organism, i.e., mobilization of energy. [56, 73, 81, 82]. For example, the emotion 'sadness' is characterized by a negative valence with a moderate level of arousal [73]. Overall, while emotion theories differ in their processes and terminology, they share a common thread in describing emotions caused by the interpretation of previous experiences and bodily states to prepare for action [8, 57].

Following, we define emotions as mental states resulting from the anticipation of emotional responses that are based on previous emotional experience, the current interpretation of bodily states, perceptions, and environmental cues (e.g., the experience of incidents in the past and cues that are similar in the current state; termed "causes"). They serve the purpose of guiding an individual's action and aiding in prioritizing and organizing behaviors to adapt to environmental demands (e.g., prevention of cognitive overload or maintaining social acceptance; termed "consequences"). Therefore, when analysing emotions in cybersecurity, it is essential to consider their causes and consequences at the same time.

2.2 Emotions in Cybersecurity

Emotions. Most emotion research in the field of cybersecurity derives specific emotions from related fields such as IT usage [22]. Here, studies predominately examine the effect of fear, sadness, or anxiety, mostly using quantitative methods to capture emotions [1, 22, 25, 59]. Furthermore, some research

faces challenges in precisely defining emotion terms, leading to difficulties in adequately capturing emotions [88].

Causes. Current research on the causes of cybersecurity-related emotions is fragmented. Identified causes include cybersecurity incidents [6,21], employer error management [77], the relationship of users and professionals [63], security notifications [29] and persuasive strategies in cybersecurity awareness and education [35,45,89].

Consequences. Initial studies identify emotions and affect as central drivers of behavior within cybersecurity. Studies, for instance, indicate that positive emotions display mixed behavioral tendencies [16,22], with some emotions, notably interest, playing a constructive role in promoting preventive cybersecurity behavior. Other positive emotions such as happiness, as a state of contentment with the current situation, can result in decreased precaution-taking [22]. Negative emotions, in contrast, tend to lead to less favorable behavioral tendencies, often manifesting in avoidance strategies [1, 16, 22]. Yet, results prove to be heterogeneous. While fear has been identified as a deterrent to precaution taking, anxiety may promote favorable cybersecurity behavior such as information-seeking behavior, contributing to an overall sense of precaution [6, 22, 25]. Similarly, research shows that 'shame' prompts negative actions while 'guilt' can foster self-acceptance and learning [77].

These contradictory results are particularly highlighted when considering induced emotions. Studies show that positive emotional appeals are more effective in promoting stronger password practices compared to negative appeals [45]. Inducing negative emotions such as with fear appeals demonstrate short-term positive effects on security behavior only if coupled with additional factors such as the strengthening of self-efficacy. Nevertheless, despite the eventual positive short-term impact, fear appeals may evoke negative emotions like fear or sadness towards cybersecurity overall that may result in avoidance, decreased well-being, or fear fatigue in the long-term [35, 75, 89]. While research on the consequences of emotions beyond cybersecurity behavior is limited, there are studies demonstrating that negative emotions in cybersecurity contribute to phenomena like cybersecurity fatigue and burnout [30, 72].

Despite the growing interest in emotions within cybersecurity, existing findings display heterogeneity and limitations in capturing the full spectrum of emotions. Furthermore, a holistic understanding of causes and consequences including emotional spill-over effects as a result of cybersecurity-related emotions is currently lacking. Our study addresses this gap by applying a holistic qualitative approach that includes multi-faceted emotion-related measures to unravel the complexity of cybersecurity emotions and their related causes and consequences. Furthermore, we build on the established circumplex model of affect [73] to structure our findings in a meaningful way to inform measures targeted at cybersecurity emotions.

3 Method

The study employed a multi-modal approach, combining semi-structured in-depth interviews and a qualitative survey with overall N=138 participants. This approach allows for qualitatively addressing the complexity of the research topic while exploring emotions with a large number of employees. According to the theory of constructed emotions, verbal reports are essential for assessing the content of subjective emotional experiences as objective measures cannot serve as proxies for emotional experiences [74]. Qualitative surveys complement interviews by mitigating the influence of potential interviewer effects [55]. This strategy aims to overcome the limitations associated with existing research zooming in on a few emotions and the limitations of single methods [74].

3.1 Participants

As we aimed to capture diverse organizational settings, thereby mitigating potential influences of company culture, our recruiting strategy pursued an employee sample of maximum variation including experts' as well as employees' perspectives [68]. We controlled for employee age, cybersecurity background (cybersecurity incident experience, knowledge, attitude, behavior) and organisational background (industry, function, level, security culture). For the interviews, emotional intelligence (EI) was measured to ensure participant's capability to reflect, express and discuss emotions. For details on the variables captured in each study, refer to Appendices B and C. For the recruiting, professionals from different business departments, varying across ranks and industries were approached via participant mailing lists, word-of-mouth, social media (facebook, linkedin, reddit), personal contacts, and snowballing for both the interview and survey. Participants engaged voluntarily and were not financially remunerated for their contributions. Age and work experience were collected in categories to ensure participant's privacy (please refer to 3.3 for a detailed description of ethical aspects).

Qualitative Survey. Our qualitative survey involved 112 participants across at least 18 industries, with 32 identifying as female, 78 as male and 2 as non-binary, varying in age from 18 to 64, and spanning diverse company sizes from 1 to over 1000 employees (referred to as "S_P01-112"). Table 4 shows the comprehensive sample and screening information.

Interview study. The interview study sample consisted of 26 participants of whom 11 identified as female and 15 as male, varying in age from 18 to 64. The sample covered 12 industries with a work experience ranging from 1 to 40 years (referred to as "I_P01-26"). On a seven-point scale, participants rated their IT-expertise with $M = 4.45$ ($SD = 1.30$) and cybersecurity-expertise with $M = 3.77$ ($SD = 1.34$). Data collection was stopped as soon as theoretical saturation was reached [44]. For comprehensive sample information including the sample screening see Table 2.

3.2 Study procedure

Qualitative Survey. For screening of the sample, participants' cybersecurity attitude (SA-6; [39]) and behavioral intention was measured (SeBIS; [36]). Then, participants provided consent and reflected on their (1) emotions towards cybersecurity, (2) thoughts on cybersecurity, (3) cyberattack incident experiences, and provided (4) demographic data. Please refer to Appendix C for detailed information on the survey.

Interviews. Due to the emotion-related nature of this research, physical and psychological safety was considered by informing participants in advance that they were to participate virtually from a safe location and by ensuring that all data was kept confidential to create a comfortable atmosphere that would increase trust and thus to increase the willingness to share information [61]. During the interviews, we used miro - a digital whiteboard - to capture relevant information onto a prepared template, so that the interviewer and interviewee could refer to it throughout the interview. The interview length ranged from 0:24 to 1:27 hours (M = 0:52). Before the interview each participant was informed about the objectives, procedures, and data processing of the study and provided informed consent (see Ethical Considerations). Furthermore, for the screening before the interview, they filled out a survey, in which their demographic data was collected first. Then, the survey asked for emotional intelligence using the self-rated emotional intelligence scale [87]. Regarding cybersecurity, knowledge, attitudes and behavior were assessed using an excerpt from the Human Aspects of Information Security Questionnaire (areas from HAIS-Q: password management, email use, internet use) [66] and the climate about cybersecurity was recorded using the Information Security Climate Index (ISCI) [52].

The interview guide was divided into four focus areas detailed in Appendix B:

1) *Emotions towards cybersecurity.* The first focus area aimed to examine emotions towards the general term 'cybersecurity' and its specific areas. Participants were first familiarized with the subject and with the verbalization of emotions by reflecting intuitively on their emotions towards cybersecurity and the relevance of the term 'cybersecurity' in their everyday work. All mentioned emotions were visualized in an emotion-overview in miro. Then, a definition of 'cybersecurity' was introduced to establish a common understanding.

1.a) *General term of cybersecurity.* For a common understanding of the previously described emotions, the participants were presented the non-verbal Product Emotion Measurement Instrument (PrEmo), depicting 14 (7 positive, 7 negative) emotions as cartoons in its second version, to enable participants to reflect thoroughly on their emotions towards cybersecurity [33, 34]. When using the PrEmo, interviewees were instructed to use the tool to help them identify their emotions towards 'cybersecurity' by the use of non-verbal depictions. Thereafter, participants were asked to reflect on the meaning and perceived intensity on a continuous scale ranging from low to high. To ensure a common understanding, participants were then asked to name the chosen emotion, if possible. After the discussion of the PrEmo, participants were asked to add any further emotions they feel towards cybersecurity, which were not included in the PrEmo. For this, an emotion word list was added to the whiteboard for the supplementation phase after using the PrEmo to facilitate verbalization of emotions that are felt but could not be named ad hoc. For details, see additional digital appendix B (linked in Appendix A). For the creation of the word list, literature was screened for emotions connected with cybersecurity, IT-usage, user experience and basic emotions in general. The number of positively (30) and negatively (30) valenced emotions was balanced and further neutral items (5) were added resulting in a total of 65 emotions. Participants were asked to select three emotions from the prepared word list that best describe their general feelings toward cybersecurity. Both verbal and non-verbal tools were used to help articulate emotions, but participants were not limited to these tools.

1.b) *Specific areas of cybersecurity.* Multiple cybersecurity areas could elicit a variation in emotions (e.g., emotions towards precaution behavior might be different from emotions elicited by a cybersecurity incident) [78] and, thus, influence overall emotions towards cybersecurity. To gain an understanding of emotional experiences influencing the overall emotions towards cybersecurity, we added a section in which participants were asked to reflect on multiple areas within cybersecurity. For this, areas were derived from the user-centered aspects of the NIST framework and visualized in a template on the miro-board [64] However, as capturing emotions retrospectively carries the risk of recall errors and exposes rationalization, a narrative interview section on the main areas was included to encourage participants to rely on their episodic memory [53]. Consequently, participants were guided to reflect in a free narration on their emotional experience within the pre-defined cybersecurity areas, if existent. These emotions were discussed and, if desired, added to the emotion-overview.

2) *Causes and consequences of emotions.* Before delving into the focus area, participants were asked to decide on three emotions that best describe their emotions towards cybersecurity overall. Based on these, we aimed to capture the causes and consequences of participants' emotions towards cybersecurity as a general term. To trigger a change of perspective, a miracle question was additionally used. These questions originate from therapeutic practices, aiming to envision a preferred future rather than holding on to past problems, while encouraging positive changes. Interviewees are asked to imagine how their life would be different if a miracle happened overnight, allowing them to reflect on current shortcomings and needs [32]. Consequences of these three emotions were further asked on both primary (everyday-work) and secondary (cybersecurity) tasks.

3) *Coping.* In the third focus area, we asked participants to reflect on what strategies they use for emotion regulation. We considered intra-individual strategies and strategies of the individual on the part of the company.

4) *Emotions within situational self-efficacy.* The final focus area examined the interdependence of emotions and self-efficacy. Participants were asked to rank their cybersecurity self-efficacy on a scale and describe their reasoning.

3.3 Ethical Considerations

The studies had been reviewed by the independent ethics committee of one author's institution and had been designed to comply with established guidelines for research involving humans [5]. Before both studies, participants were informed about the study's purpose, structure, conditions and data processing, with a clear emphasis on voluntary participation and the right to withdraw without consequences. Participants were informed that participation was voluntary, that they had the right to quit the study at any time without negative consequences and ultimately were asked to read the consent form including the study's data protection policy and give consent. To enhance privacy, we reduced the collection of personal data to a minimum and abstract categories were used. After the interview, each participant received a random identifier for confidentiality, and data were stored on servers complying with national privacy regulations. Overall, the study ensured compliance with national privacy regulations. Considering the potential for participants to share distressing cybersecurity experiences (e.g., feeling ashamed as a result of falling for a phishing email or suffering serious losses due to a cyberattack), interviewers were prepared to handle strong emotions. Interviews could be paused or terminated if necessary, and participants were offered the opportunity to be referred to an appropriate office via the research supervisor for ongoing concerns after the interview.

3.4 Data analysis

All interviews were first transcribed and then analyzed using thematic analysis [19]. As the analysis of complex data benefits from the interaction between coders, multiple interaction and alignment phases were included [65]. First, two coders individually analyzed 20% of the data set that were randomly chosen to derive an initial codebook. Going back and forth several times, a codebook was iteratively developed. A final codebook was formed from discussion and continuous refinement, based on which one researcher coded the complete dataset while aligning with the second coder on the progress multiple times. This approach follows the recommendations for thematic analysis, which advices against multiple independent codings and calculating inter-coder reliability [26]. In the identification of emotions, we also considered terms that are rather cognitive states, feelings, or evaluations (as seen

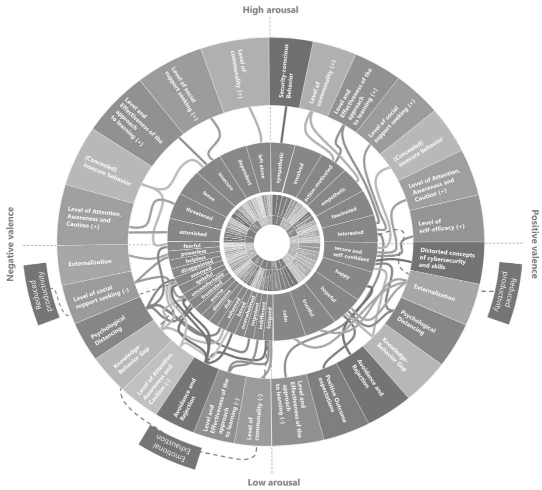


Figure 1: Eye of cybersecurity-related emotions. See digital appendix A (linked in Appendix A) for a larger color version.

in [31]), and, hence, are not emotions as per definition. Yet, as multiple participants used these terms to describe their emotions, reflecting the subjective and varied nature of emotional experiences in their language and understanding, we integrate terms that are related to emotions (e.g., 'secure'). We omitted participants who expressed emotions related to work-related matters rather than those specifically to cybersecurity.

In a second step, to analyze dependencies, i.e., code configurations of causes, consequences and emotions, we analyzed joint appearances of codes assigned to emotion + consequences or emotion + causes, e.g., exemplary code for cause + emotion: *"Countless passwords. That annoys me. (I_P21)"*.

In a third step, we applied the circumplex model of affect to structure the identified emotions into four classifications (high-low arousal, positive-negative valence) [73]. These classifications were further used for a document-wise reflection on the occurrence of *mixed* emotions across participants.

4 Results

The following sections first introduce the identified emotions with cybersecurity and then describe findings related to the *causes* and the *consequences* of these emotions. Figure 1 provides an illustration of all coded emotions, contextualized in a circumplex model, and their relation to the causes and consequences. Afterward, Figure 2 provides an overview of the underlying framework and the identified emotions, causes, and consequences that align with the section's subheadings.

Following Braun & Clarke's [20] recommendation for reporting results of a thematic analysis, we portray the results of our two studies, provide illustrative quotes and discuss them

directly where applicable. For further quotes, the reader is referred to the codebook in the additional digital Appendix F (number given in brackets (#number)). To avoid the appearance of generalizability and quantification of the answers and to emphasize the depth of the qualitative data, we do not give exact ratios, but instead approximate proportions [20]. Themes and codes that occurred more frequently are provided in descending order.

4.1 Emotions in Cybersecurity

The circumplex model categorizes emotions along the two dimensions: valence (negative - positive) and arousal (low - high) [73]. Overall, participants described more negative than positive emotions with cybersecurity. For positive emotions, participants primarily stated that they feel 'interested', 'secure' (often including feeling self-confident), and 'happy'. For negative emotions, almost all participants stated feeling 'annoyed', whereas almost half of the participants described feeling 'insecure' or 'dependent'. Some participants described emotions that were neither positive nor negative, e.g., being unsure how to feel about the topic. Participants generally described more low-arousal emotions (e.g., 'annoyed', 'uncomfortable' or 'happy'), compared to high-arousal emotions (e.g., 'insecure', 'tense' or 'interested'). For all coded emotions, refer to the gray circle in Figure 1. Almost all participants experienced mixed emotions. For most participants, multiple or all emotion classifications appeared simultaneously (see additional digital appendix E).

4.2 Causes of Emotions in Cybersecurity

4.2.1 Individual Factors: Personal Perceptions

Level of Knowledge and Experience. All participants acknowledged that their level of knowledge and experience influences their emotions toward cybersecurity. The level of knowledge included understanding specific aspects and the general concept of cybersecurity. One person, for example, expressed requiring more knowledge without being able to specify it (#3).

Regarding experience, firstly, emotions were influenced by life experiences, as highlighted by one participant: *"I've been working with computers for about 40 years, and because I've already dealt with many passwords and various things. (I_P11)"*). Secondly, the introduction of new measures or routines triggered emotions (#8), in particular, the experience of receiving suspicious emails (#9). Some noted that emotions tend to become more positive over time with increased experience or routine.

Perceived Level of Protection (active). Many participants reported that their subjective personal engagement and their perceived cybersecurity abilities influenced their emotions (#10). Here, several participants expressed a commitment to self-defined areas of impact, that do not necessarily align with actual protection levels.

Perceived Lack of Autonomy. Half of the participants expressed limited self-determination in cybersecurity. Specifically, participants felt restricted or coerced by cybersecurity requirements (#11), with some feeling patronized as they lacked the autonomy to decide on the procedure and options of their protection strategy, e.g., time of an update or use of measures such as passwords or biometric authentication: *"I don't have any freedom of choice, I'm just dependent on the arbitrary order to do it that way. (I_P21)"*. Other participants stated that they felt their freedom and rights were generally being curtailed: *"It's a narrative that cybersecurity is an insecure restriction of personal rights. (I_P17)"*.

Internal Conflicts. Most participants expressed internal conflicts involving contradicting attitudes, beliefs, or perceptions. Many described seeing the world as a safe place and a desire to trustfully engage with their environment [27], while simultaneously feeling pressured to adopt a general sense of distrust and experiencing betrayal by individuals they wish to trust. One participant noted: *"I realize that's just the way it is in today's world. You have to be vigilant, you have to be attentive and you have to learn to deal with it. [...] I accept it for myself, even though I don't always like it. (I_P21)"*. Other participants noted a conflict between disinterest and acknowledging cybersecurity's importance or they recognized a discrepancy between their desired and actual engagement in certain behaviors impacting their emotional state.

Perceived Vulnerability. Many participants also reflected on their vulnerability (#15), concerning both, the perceived vulnerability of their company and themselves resulting from behavioral tendencies. Participants often reflected on the extent to which an attack on the company is coincidental to the level of protection (#16).

Anticipated Consequences. The impact of anticipated consequences on participants' emotions varied in terms of the level of abstraction, awareness, and focus. While some reported concrete anticipated consequences, such as business continuity, others depicted rather abstract consequences with far-reaching consequences (#17). Additionally, some participants reflected on the subject of the anticipated consequences being themselves (#19).

Perceived Value of Data. Participants noted that their perception of handled data influences their emotions. In particular, the interviewees reflected on the level of sensitivity of the company's data (#20).

4.2.2 Individual Factors: Cybersecurity Perceptions

Perceived Narrative and Relevance. The participants varied in their perception of cybersecurity's relevance. Many interviewees acknowledged its significance or omnipresence in both their professional and private context (#21). Participants approached cybersecurity from diverse viewpoints, reflecting

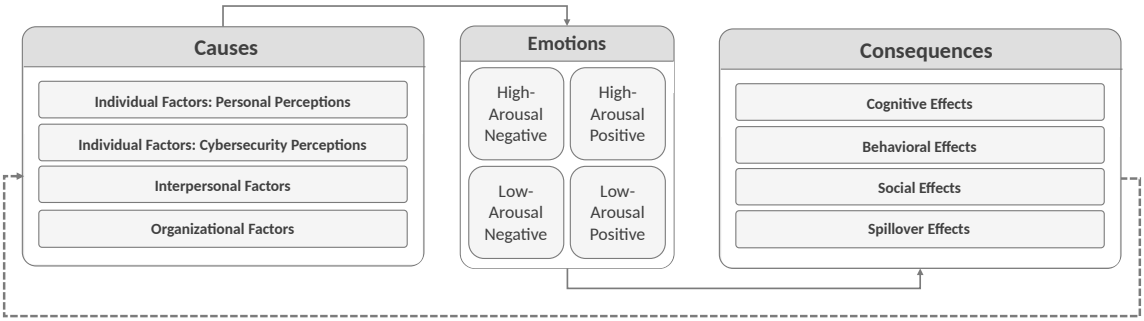


Figure 2: Framework of emotions in cybersecurity

on it both within the context of their company's processes and measures (e.g., password security requirements) and from a broader perspective (e.g., from the point of view of hackers, reporting on attacks, cybersecurity in technical progress): *"On the one hand, I would just be so disinterested when it comes to cybersecurity, but I find that then again I'm interested in how something like that takes place when it comes to things like that, how hackers go about it. (I_P03)"*.

Perceived Resource-Intensiveness and Hindrance. Over half of the participants view cybersecurity as a hindrance or cumbersome to their workflow.They highlighted processes that are perceived as time-consuming or are required at inconvenient times (#24), e.g., password requirements and regular password changes. Furthermore, some participants described a trade-off between security and usability (#23).

Perceived Level of Control. Many participants reflected on their ability to control the possible consequences of cybersecurity attacks, but also on the reliability of security measures which impacts their emotions towards cybersecurity. Some participants delineated aspects where they perceived being able to exert control. Simultaneously, they expressed the limitation of one's influence beyond this defined scope, for example, attacks from unknown parties (#25, 26). The described aspects were often arbitrary and limited to simple basic measures (e.g., locking screens when leaving their workplace). At the same time, some participants described how their own skills are uncontrollable to a certain extent, e.g., influenced by the form of the day, identity or human curiosity: *"I can't do that. [...] I'm not an IT professional. (I_P20)"*. Furthermore, some participants described having only limited influence on preventing an attack among the mass of employees, for example: *"I don't know how many employees we have and yes, my influence is relatively small. (I_P18)"*.

Perceived Level of Necessity. Participants reported different levels of perceived necessity about undertaking cybersecurity measures, e.g. confusion about the purpose of a measure: *"I'm not going to do it. I refused the measure. Out of no understanding of the necessity. (I_P15)")*. Other perceived cybersecurity measures as *"a necessary evil (I_P24)"*. Some participants described how they feel engaging in cybersecurity is necessary, while others feel that measures are excessive and unnecessary. Some participants generalized this feeling from one measure to the entire concept of cybersecurity.

Perceived Complexity. Some participants outlined that they perceive cybersecurity as such a complex and dull topic that it can only be grasped to a limited extent by everyday users. This perception is similar to parts of the cybersecurity perceptions described by Haney et al. [47]. They also mentioned many technical terms used in the field that are not explained. Some participants also described that no matter how much they learn, there is always more to learn (#31).

Media Reports as Trigger for Cybersecurity Perceptions. Across all individual factors, media reporting was described as the most influential factor for perceptions and, thus, emotions towards cybersecurity. Participants described cybersecurity being portrayed as a negative term with far-reaching consequences for humanity (#32). Some participants outlined that reporting on attacks by related companies in particular triggers emotions.

4.2.3 Interpersonal factors

Self-perception and Perception of Others. Among the most frequently discussed causes for emotions were firstly, the anticipated perception of oneself through colleagues due to cybersecurity behavior or attitudes and secondly, perceptions of colleague's cybersecurity behavior and attitudes. Many participants noted that most colleagues exhibit a low priority for cybersecurity, displaying negative attitudes, substantial knowledge gaps, and insecure behaviors, e.g.,*"When I hear the word cybersecurity, the first thing that comes to mind is naivety and stupidity. [...] I also think of ignorance and carelessness. (S_P69)"*. Yet, some participants emphasized sharing the same feeling about cybersecurity with their colleagues. At the same time, many participants expressed concerns about possible negative evaluations such as being seen as paranoid or spoilsports, when exhibiting safe behavior, e.g., *"Maybe I just don't want to describe myself as paranoid.*

(I_P18)"). Furthermore, they worried that their actions may seem inconsistent with their social identity, e.g., *"Sometimes I'm embarrassed about myself, in the sense of what kind of background [IT background] I actually have, whether others know that. How others think about me. [...I] could do better (I_P25)"*). Generational differences in growing up with digital technologies and the subsequent evaluation of one's own and other generations were commonly highlighted (#38, 39).

Level of Social Exchange. While some participants described that the exchange about cybersecurity is an essential part of their work life, the majority expressed a reluctance to talk about cybersecurity. Also, they expressed that others are similarly disinterested in such discussions, e.g., *"Never talked about it, never had the feeling that there was a mood. (I_P20)"*. Yet, many participants noted that they were generally willing to talk about cybersecurity under favorable conditions or when initiated by others.

Perceived Relationship with Experts. More than half of the participants portrayed interpersonal factors shaping the relationship between employees and security experts (or IT department), ultimately influencing emotions in cybersecurity. Participants frequently noted hindered communication characterized by a lack of proactive communication between the two parties, with contacts often initiated in response to negative events (#41). Moreover, they outlined that communication styles including IT-jargon and lengthy explanations, or slow response times create a disconnect with the security department. Other participants perceived being patronized by security experts, akin to the treatment of children: *"Sometimes you really are treated like a small child who just doesn't know how the Internet works yet. (I_P10)"*; *"I think that's more like bullying. (I_P11)"*. Overall, employees expressed feeling undervalued or unappreciated in their efforts and described that their needs are not met. This theme confirms results by Menges et al. [63] showing a dysfunctional relationship between users and experts characterized by particularly negative feelings towards each other, negativity in communication, emotional disengagement and blaming.

4.2.4 Organizational factors

Perceived Level of Protection (passive). While "perceived level of protection (active)" (see section 4.1.1) considers actively taken actions, this theme encompasses actions taken by the company, including technical solutions, availability of policies, and expert support. Many participants articulated the level of trust in the technical solutions provided by their company allowing them to focus on their daily tasks. They also portrayed views on the structural availability of security strategies, reflecting on support options and the overall presence of experts in their infrastructure (#44).

Perception of Design and Frequency of Education. Another subtheme centered around the design and frequency of cybersecurity education, including training materials, communication, or awareness campaigns. Views on the frequency of educational initiatives varied: Some had a negative perception, especially when content was repetitive, e.g.,: *"I'm annoyed because [...] some things don't need to be told ten times, we know them. (I_P11)"*. This sentiment led to a perceived lack of being taken seriously and a sense of distance from security experts. Some also noted challenges with the complexity of the content and its practical application. Others appreciated frequent training. Notably, some highlighted the importance of their colleagues undergoing training, particularly due to unsafe behavior. Preferences regarding content varied, with some desiring more exciting and fun content, while others questioned the effectiveness of gamification. They expressed a preference of "serious" but well-prepared materials, in particular, due to the seriousness of the topic.

Perceived Security Culture. The perceived importance of security within the company and among colleagues and the priorities by management, shaped participants' perceptions of cybersecurity responsibility at both the team and organizational levels. Some participants felt pressured to adhere to unspoken, potentially insecure guidelines, feeling expectations from colleagues or managers, to conform to such practices, e.g., *"So there are already gray areas being entered to get it done. Then it doesn't matter at that moment. Be it that we break data protection regulations. (I_P22)"*.

Perceived Demands and Requirements. Several participants discussed the burden and practicability of security requirements imposed upon them. Many found security measures and regulations overwhelming and, at times, impractical. While some referred to explicit requirements outlined in policies, others sensed unspoken agreements and expectations that may not align with official security policies (#50).

Error Culture. Many participants referred to the company's error culture, highlighting concerns related to a shaming and blaming culture in the organization, where mistakes are not openly addressed and blamed even if unintentional. Some participants described a secretive organizational culture with no opportunity to learn from others' mistakes: *"But how am I supposed to learn from mistakes if I'm not told about them? (I_P14)"*. Others describe a positive error culture encouraging open discussions about, promoting reporting without fear of reprisal, and prioritizing learning.

4.3 Consequences of Emotions in Cybersecurity

4.3.1 Cognitive Effects

Psychological Distancing and Repression. More than half of the participants showed an unconscious cognitive or emotional separation from the term cybersecurity or consciously suppressed the topic (#52). Distancing oneself from the topic causes disconnection and is associated with a deactivation of positive behavioral tendencies as investigated in the context

of precaution taking [22].

Externalization. Around half of the participants externalized their cybersecurity responsibility, attributing it to their peers, management, security experts, or third-party companies, e.g. for initiating communication and education. On a structural level, many participants demanded or selected technical solutions as a means to abandoning personal responsibility. Some participants described that people with greater expertise should deal with the topic, positioning themselves in a more passive role, e.g., *"I rely on my employer to protect his company. (S_P85)"*.

Distorted Concepts of Cybersecurity and Skills. Some participants narrowed cybersecurity to specific actions, such as avoiding phishing emails, leading to spill-over confidence in broader cybersecurity capabilities. This selective attention contributes to the overestimation of one's overall cybersecurity skills. Furthermore, the impact of incremental improvements is often overestimated (#55).

Level of Self-efficacy. Participants described that their emotions influenced their level of self-efficacy. Nonetheless, a direct connection to emotions was not explicitly articulated (#56). Overall, self-efficacy is known to be highly influenced by emotions [9].

Positive Outcome Expectations. A few participants tended towards convincing themselves of a positive overall situation, and that nothing would happen to them or their company. However, no measures are being taken to ensure that this positive scenario actually occurs. Some showed a tendency to believe that they in comparison to others would be less susceptible to future cyberattacks (e.g. optimism bias, [79, 85]), e.g., *"You know it's somehow not ideal and I hope that nothing will go wrong anyway. (I_P18)"*. This stance is similar to wishful thinking, a belief that is rather based on an individual's desire than actual evidence or rational analysis [14], or optimism bias, a bias underestimating the likelihood of experiencing negative events [18]. Both of which are known to be highly influenced by emotions and investigated in the context of cybersecurity [24, 48]. Yet, optimism bias is known to be independent of cybersecurity education [48].

4.3.2 Behavioral Effects

Level of Attention, Awareness and Caution. Most participants described a shift in the level of their attention between either focusing on a specific area of interest (e.g., potentially harmful emails) or undirected, general attention as a preventative measure without associated measures (#58).

Level and Effectiveness of the Approach to Learning. Half of the participants reflected on the impact of emotions on their willingness and effectiveness to learn. While some described that they actively seek information, others explicitly stated to not seek information. Furthermore, participants outlined the emotion's effect on the effectiveness of learning or retrieving information when needed (#59). Prior research also demonstrated a major effect of emotions on learning, recall, and the effectiveness of academic learning [69].

Avoidance and Rejection. This theme, in contrast to Psychological Distancing and Repression, involves proactive and conscious measures to evade (aspects of) cybersecurity. Half of the participants described that a range of emotions contributes to their avoidance and rejection of specific cybersecurity measures or overall cybersecurity, eventually resulting in a sense of resignation, e.g. *"[This leads to] me not wanting to deal with the issue. And generally not wanting to have anything to do with it (I_P03)"*.

Knowledge-Behavior Gap. Approximately half of the participants admit to not consistently following cybersecurity guidelines, despite being aware of their importance. Some name potential solutions, yet, hesitate to adopt them, e.g., *"I know what these passwords should look like. [...] I usually use a password that I can remember well.[...] Not the super secure ones, I'll admit that. (I_P12)"*.

Security-conscious Behavior. Participants described how cybersecurity had become part of their routine, expressing specific behavioral tendencies or reporting anomalies (#63).

(Concealed) Insecure Behavior. Some participants described engaging in practices that are conducted outside the official security policies of their organization or find workarounds to the company's requirements, yet, are seemingly security-conscious (e.g., having a strong password, but written down: *"I have my file where I write it down. [...] I don't have them all saved in my head (I_P21)"*). In contrast, other participants openly pursue insecure behavior. These behaviors are in line with tendencies revealed by Beris at al. [16] as a consequence of affect.

4.3.3 Social Effects

Level of Social Support Seeking. Participants varied in their active pursuit or desire of social support. This phenomenon includes seeking emotional support, e.g., venting, in line with [59]. An example was: *"When I'm really angry, I can also vent my anger in our office. Then I always get approval. If you're angry, you're not angry alone. [...] And then I'm doing quite well (I_P16)"*. Outward emotion-focused coping, i.e. venting, is associated with increased levels of desirable security behaviors [59]. Some participants, exhibiting low levels of seeking social support, expressed concerns about being perceived negatively, e.g., as paranoid, by others: *"Nowadays, when I say IT or cybersecurity, it has a negative connotation. And that's why I try to avoid the term (I_P14)"*).

Level of Communality. The level of communality is the degree of active support among colleagues. Some participants described actively approaching colleagues to share their knowledge and to work together on cybersecurity (#67). Others described deliberately hiding their knowledge, which has been observed for the interaction between users with high and low cybersecurity expertise [43].

4.3.4 Spillover Effects

Emotional Exhaustion. More than half of the participants described that their emotions towards cybersecurity had far-reaching effects, manifesting in feelings of fear, avoidance of certain topics or tasks, and an overarching sense of burden. One participant noted: *"Sooner or later, it ensures that if this emotion were permanent it would turn into a kind of aversion and therefore the measures are not implemented. (I_P15)"*. Fear, particularly, is seen as a constraint in personal growth (#69). Negative emotions led to prioritization of enjoyable activities over tasks evoking negative emotions. One participant stated: *"Life [without cybersecurity] would be easier, there would be less stress and certainly less burnout at work. (I_P14)"*. A few participants described negative feelings towards their employer: *"Of course, I'm also angry at my employer for constantly making life difficult for me. (I_P13)"*. Dupuis et al. [35] propose that the evocation of negative emotions can generally have negative effects on well-being or job satisfaction. Our results support and extend these findings by showing effects on far-reaching areas of life and that negative experiences (inclusive cybersecurity) are actively avoided.

Reduced Productivity. Participants highlighted that their emotions towards cybersecurity had an impact on their daily productivity, affecting primary work tasks or adopting new technologies. They felt frustrated and annoyed with the constant need to be vigilant and check for phishing emails, at times, leading to ignoring or directly deleting potentially important mails, e.g., *"If I'm not expecting an email, then I don't pay attention to the emails. [...] And if someone really has something important, they can either send me another email or call me. (I_P12)"*.

Need for Recovery. Some participants articulated a need for a timeout as a consequence of negative emotions caused by cybersecurity (#74). Beyond discontinuing their working task, they suggested various methods for recovery, such as disconnecting from technology, going for walks in nature, and engaging in hobbies or activities that provide relaxation and distraction. Despite the short-term impact, some participants noted that emotions arising from colleagues' non-favorable cybersecurity behavior significantly influenced the decision to changing workplaces.

4.4 Contextualization of Findings: The Circumplex Model of Cybersecurity Emotions

Using the circumplex model of emotions, the following sections bring together identified emotions related to their causes and consequences as illustrated in Figure 1.

4.4.1 Identified Cybersecurity Emotions

Causes of cybersecurity-related emotions are displayed as the inner circle and consequences are visualized on the outer circle within the eye of cybersecurity-related emotions in Figure 1. To illustrate the relationships between emotions and their consequences, paths are depicted in Figure 1 while paths for causes-emotions were excluded for better legibility. In the interest of clarity, pathways for causes-emotions were omitted. Please refer to Table 1 for detailed occurrence patterns of the observed interplay of causes-emotions-consequences. For instance, for a low-arousal negative emotion: a *low level knowledge*, *high anticipated consequences* and *negative self-perception or perception of others* resulted in feeling *fearful* and, thus, *psychological distancing* and *(concealed) insecure behavior* or for a an exemplary path for a low-arousal positive emotion: a *high level of perceived protection (active)*, a *high level of perceived control*, a *high level of perceived protection (passive)* and the perception of the organizational *security culture* leads to *happiness* and consequently, in line with Burns et al. [22] *avoidance and rejection* behaviors.

As expected based on the circumplex model of affect, low-arousal emotions were associated with states of low or no action including psychological distancing, avoidance and rejection, and a knowledge-behavior gap. Similarly, low-arousal but positive emotions were linked to psychological distancing, a knowledge-behavior gap, or externalization. Conversely, high-arousal emotions led to a higher activation, particularly increased levels of communality, and higher effectiveness of the approach to learning (see Figure 1). Yet, both high-arousal classifications risk an increased level of (concealed) insecure behavior (particularly for insecurity, fear, and interest).

In contrast to previous results [22], 'interest' was associated with positive and negative behavioral tendencies as well as consequences actually connected to low-arousal emotions (e.g., a decreased level and effectiveness of the approach to learning) and feeling 'secure' (often including feeling self-confident) which resulted in misconceptions or (concealed) insecure behavior. The unfavorable effect of 'interest' can be partially explained by the forced-compliance paradigm that predicts that individuals required to comply with a task perceived as boring experience cognitive dissonance. Thus, as humans strive for balance, they need to balance out the dissonance either by discontinuing or reassessing the perception of the task [40]. Discontinuing is no attractive option as there is a risk of maintaining one's self-image and perception by others Instead, re-evaluating the task helps maintain self-preservation.

Unlike Beris et al. [16], who identified negative behavioral tendencies for negative affect and mixed behavioral tendencies for positive affect, our results demonstrate both behavioral tendencies for both positive and negative affect. This might be because we considered further behavioral tendencies exceeding compliance. Our results reveal that high-arousal negative emotions have no direct positive effect on behavioral tendencies, but display indirect positive effects such as increased information and social support seeking. Yet, in line with the authors' results, our work shows that employees pursue behaviors that might be seemingly secure. In line with

Renaud et al. [77], we found that shame results in undesirable behavioral tendencies.

Considering spillover consequences, low-arousal emotions with a negative valence resulted in overall reduced productivity and emotional exhaustion. 'Interest' was the only positive emotion that was linked to reduced productivity. Please refer to Figure 1 for an illustration of the interconnections between emotions and consequences.

4.4.2 Mixed Emotions

Despite varying backgrounds, including a variation in knowledge or industry, participants display mixed behavioral and cognitive tendencies of favorable and unfavorable nature. Thus, multiple behavioral tendencies and occasionally contradicting cognitions are present simultaneously stemming from emotional dissonance. For example, participants feel interested in cybersecurity and would like to learn more about it, still, they are afraid of being judged by their colleagues and avoid the topic overall. Another illustrative example: Some participants are knowledgeable, feel secure and would like to engage in secure behavior, yet, feel patronized by security education and consciously act against guidelines. For an details on the document-wise assignment of codes, see digital Appendix E.

5 Discussion

5.1 Summary of Key Results

Overall, our findings shed light on the role of emotions in cybersecurity by highlighting causes, types and consequences of emotions. Delving into the causes of cybersecurity, our study expands upon prior research [45, 63, 77] by categorizing examined factors in four themes: individual personal perceptions, individual cybersecurity perceptions, interpersonal, and organization-wide factors. While existing literature predominantly focuses on negative emotions such as fear, sadness [1, 6, 89], often derived from related areas such as IT usage [22], our exploratory approach presents a comprehensive perspective on the emotions towards cybersecurity. Indeed, feelings of fear and insecurity were highly prevalent, yet, only a small share of the experienced emotions towards cybersecurity overall. While previous research often considered the experience of one single uniform emotion [16, 22, 25], our research reveals the simultaneous occurrence of multiple contradicting emotions in most individuals. This also supports the theory of constructed emotions, explaining the diverse and complex emotions reported, influenced by personal, social, and organizational factors in cybersecurity. While previous research primarily considered behavioral tendencies including precaution behavior, compliance, and emotional coping behavior [16, 22, 25, 59], our results confirm and extend them by revealing a complex interplay of multiple behavioral, cognitive, and social consequences simultaneously. Furthermore, we show that emotions towards cybersecurity spill-over to other areas of life: some individuals feel emotionally exhausted, impeded in their productivity, or feel a need for distancing from their work in general.

5.2 Recommendations for Cybersecurity Practitioners

Overall, our findings indicate that practitioners should aim for *first* addressing emotions while reducing emotional dissonance (e.g. through the establishment of an emotion-oriented mindset). *Second*, high-arousal emotions and subsequent causes should be enhanced while considering the risk of undesirable activation i.e. *(concealed) insecure behavior* and low-arousal emotions and their subsequent causes should be diminished. We advise for a holistic strategy as emotions caused by one area can impact the overall approach to cybersecurity. This approach seeks to integrate the humans with all their complexities, into the socio-technical framework of organizational cybersecurity. Additionally, it aims to protect individuals from potential negative consequences thereby enhancing their ability to focus on their primary work task. Key components of the advised strategy are the following:

5.2.1 Establishment of an Emotion-oriented mindset

Cultivate empathy. The lack of security behavior or behavior change in general is mostly determined by the perception of emotional ambivalence [80]. Practitioners should recognize the role of emotions and establish channels for emotional support, where employees can share their emotions (anonymously), *seek social support*, foster a positive *sense of cybersecurity culture* and, thus, prevent *emotional exhaustion*. Additionally, cultivating empathy towards experts enhances the *relationship with experts*. We advise to share real-life cybersecurity stories and case studies within the organization to improve *cybersecurity perceptions* and the *expert-user relationship*. As storytelling was already shown to have positive effects on cybersecurity education [71], it might also be leveraged for cultivating empathy.

Set the stage. To mitigate internal conflicts, we recommend creating a culture of psychological safety where employees should feel empowered to ask for expectations and question tasks perceived as insecure. Acceptance of varying interest levels in cybersecurity is crucial, and enforcement strategies should be avoided to prevent suboptimal results. Instead, cybersecurity should be presented in relatable terms, portraying realistic consequences and clearly defining *areas of control*. Recognizing that some employees may perceive their impact as minimal, especially in light of colleagues' insecure behavior, it is crucial to make employees aware that everyone plays a valuable role in the company's security strategy [90].

Foster emotional reflection. While enhancing positive emotions can help overcome negative emotions, there's a potential drawback: the introduction of positive low-arousal emotions associated with undesirable behavioral tendencies. To ensure mental health and emotional resilience, it is crucial to promote emotional reflection to maintain a balanced and healthy emotional state within the cybersecurity context.

5.2.2 Enhancement of high-arousal Emotions and Diminution low-arousal Emotions

Here, we outline exemplary strategies for enhancing high-arousal and mitigating low-arousal emotions. Further strategies can be derived from Figure 1 by examining and modifying causes of low-arousal or high-arousal emotions. For instance, low levels of perceived control were identified as a cause for negative low-arousal emotions and subsequent negative consequences. Providing users with a moderate sense of control through **clear communication**, such as imparting hands-on strategies like emphasizing the importance of password length to prevent brute-force hacking, can convey a sense of control. Further, fostering an environment of transparency, it is crucial to articulate cybersecurity goals, i.e., the *area of control*, and the *necessity* of measures clearly. Employees should feel able to influence security measures such as by giving the possibility to update a software at one of two time-slots. Involving user representatives in decision-making processes enhances a sense of *autonomy* among employees. Yet, attention must be paid to strategy implementation, as high levels of perceived control can result in feelings of positive low-arousal emotions and undesired consequences.

The *level of knowledge* and expertise is a major cause of high-arousal emotions, while also posing the risk of impacting low-arousal emotions. Therefore, we advise carefully fostering high-arousal emotions and mitigating low-arousal emotions, such as through the implementation of **individualized cybersecurity education**. While some employees struggle with IT-jargon, others feel bored or coerced by repetitive or basic training (*perception of design an frequency of education*). Thus, we recommend assessing the learner's knowledge level and offering training tailored to their needs as recently proposed, e.g. by [2, 3]. Furthermore, employees prefer material that is coherent with their emotional tone and perceptions. Thus, not all employees enjoy fun or gamified training. A survey by McLauglin [62] indicates that especially leader boards decrease learning desire. Negative low-arousal emotions often stem from perceived *expertise levels*. To counteract this, we recommend developing educational material grounded in real-world scenarios. However, caution is advised as high levels of perceived expertise or the *perceived level of protection (active)* pose a risk of feeling too secure and, thus, *distorted concepts of cybersecurity*. We recommend fostering regular reflections on skills but also actually implemented measures. However, reflecting on low levels of security behavior might result in a cognitive dissonance for those with positive emotions. Hence, employees may not be blamed [77] but should be encouraged to view security behaviors as an ongoing improvement process rather than expecting instant changes. This approach mitigates the risk of cognitive dissonance resulting from the misalignment of emotions and implemented behavior. Further, employees with high knowledge or expertise levels can be impeded from openly discussing and engaging with cybersecurity due to concerns about negative perceptions from others (similar as in [43]). To address this challenge, we recommend empowering these employees by designating them as **ambassadors** and providing support to them as Gutfleisch et al. [46] illustrated that mere appointment of "security champions" without management and IT support is insufficient.

Considering the examined spill-over effects we conclude that **scaring won't do in long-term.** Despite the potential positive short-term effect of fear appeals as seen in prior research [35], scaring employees into compliance may result in fear, negative low-arousal emotions, negative effects on security behavior, the interpersonal and organizational environment and cybersecurity-related perceptions [35]. Thus, fear appeals might motivate short-term secure decisions, however, ultimately result in psychological distancing or even emotional exhaustion. To mitigate these risks, we recommend prioritizing emotional reflection over fear-based approaches.

5.3 Limitations and Future Work

While our study provides valuable insights into the interplay of emotions and cybersecurity, some limitations need to be considered. *First*, our study examined a wide range of emotions in cybersecurity but did not extensively analyze complex dependencies, such as the interplay of multiple causes or consequences of specific emotional constellations.

Second, the exploratory qualitative nature of our study limited the quantification of results. Future research could delve deeper into specific cybersecurity areas, examining emotions and their (co-)dependencies quantitatively. Adopting a mixed methods approach would benefit capturing the complex dynamics around cybersecurity emotions. *Third*, our research took a retrospective view of cybersecurity emotions, potentially overlooking temporal changes. Future research could explore how emotions evolve, e.g., in response to incidents, and their long-term impact on cybersecurity attitudes or behaviors. Further, we acknowledge that cybersecurity-related emotions might overlap with general workplace issues despite aiming for maximum variation in the sample. Our study relied on participants' cybersecurity-focused responses. Thus, future research could explore the interaction between cybersecurity and workplace culture. Future research could also investigate how strategic cybersecurity measures impact these emotions and the related consequences or behaviours, respectively or develop measurement tools that benefit from emotions capturing several causes and consequences simultaneously.

Acknowledgments

We would like to thank Anna-Maria Klein, Miriam Pitzer and Julius Klein for the support in data collection.

Data Availability Statement

Due to the high sensitivity of interview data, we do not make the interview data publicly available. Detailed information on the sample, the interview guide, code book, and exemplary quotes are provided with the article to enhance transparency and replicability. For access to the original interview transcripts, please contact the authors.

References

[1] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *Ieee Access*, 9:121916–121929, 2021.

[2] Yusuf Albayram, David Suess, Yassir Yaghzar Elidrissi, Daniel P. Rollins, and Maciej Beclawski. Personalized cybersecurity education: A mobile app proof of concept. In *HCI International 2023 – Late Breaking Posters*, Communications in Computer and Information Science, pages 257–263, Cham, 2024. Springer Nature Switzerland and Imprint Springer.

[3] S Alotaibi, Steven Furnell, and Y He. Towards a framework for the personalization of cybersecurity awareness. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 143–153. Springer, 2023.

[4] Neal M. Ashkanasy and Alana D. Dorris. Emotions in the workplace. *Annual Review of Organizational Psychology and Organizational Behavior*, 4(1):67–90, 2017.

[5] American Psychological Association. Ethical principles of psychologists and code of conduct. https://www.apa.org/ethics/code, 2023. [Online; accessed: 09-February-2024].

[6] Eric Bachura, Rohit Valecha, Rui Chen, and H Raghav Rao. The opm data breach: An investigation of shared emotional reactions on twitter. *MIS Quarterly*, 46(2), 2022.

[7] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 2015.

[8] R. P. Bagozzi, M. Gopinath, and P. U. Nyer. The role of emotions in marketing. *Journal of the Academy of Marketing Science*, 27(2):184–206, 1999.

[9] Albert Bandura. Social cognitive theory of personality. *Handbook of personality*, 2:154–96, 1999.

[10] Lisa Feldman Barrett. Solving the emotion paradox: categorization and the experience of emotion. *Personality and social psychology review : an official journal of the Society for Personality and Social Psychology, Inc*, 10(1):20–46, 2006.

[11] Lisa Feldman Barrett. The theory of constructed emotion: an active inference account of interoception and categorization. *Social Cognitive and Affective Neuroscience*, 12(1):1–23, 2017.

[12] Lisa Feldman Barrett and Christiana Westlin. Navigating the science of emotion. In *Emotion measurement*, pages 39–84. Elsevier, 2021.

[13] L. W. Barsalou. Perceptual symbol systems. *Behavioral and Brain Sciences*, 22(4):577–609; discussion 610–60, 1999.

[14] Anthony Bastardi, Eric Luis Uhlmann, and Lee Ross. Wishful thinking: Belief, desire, and the motivated evaluation of scientific evidence. *Psychological science*, 22(6):731, 2011.

[15] Christopher Beedie, Peter Terry, and Andrew Lane. Distinctions between emotion and mood. *Cognition & Emotion*, 19(6):847–878, 2005.

[16] Odette Beris, Adam Beautement, and M Angela Sasse. Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 73–84, 2015.

[17] Scott R Boss, Dennis F Galletta, Paul Benjamin Lowry, Gregory D Moody, and Peter Polak. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly*, 39(4):837–864, 2015.

[18] Anat Bracha and Donald J Brown. Affective decision making: A theory of optimism bias. *Games and Economic Behavior*, 75(1):67–80, 2012.

[19] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[20] Virginia Braun and Victoria Clarke. *Thematic analysis: A practical guide*. SAGE, Los Angeles, 2022.

[21] Sanja Budimir, Johnny RJ Fontaine, and Etienne B Roesch. Emotional experiences of cybersecurity breach victims. *Cyberpsychology, Behavior, and Social Networking*, 24(9):612–616, 2021.

[22] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4):1228–1247, 2019.

[23] Perry Carpenter and Kai Roer. *The Security Culture Playbook: An Executive Guide to Reducing Risk and Developing Your Human Defense Layer*. John Wiley & Sons, 2022.

[24] Daniel Qi Chen and Huigang Liang. Wishful thinking and it threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*, 66(4):552–567, 2019.

[25] Violet Cheung-Blunden, Kiefer Cropper, Aleesa Panis, and Kamilah Davis. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion*, 19(8):1353, 2019.

[26] Victoria Clarke and Virginia Braun. Successful qualitative research: A practical guide for beginners. *Successful qualitative research*, pages 1–400, 2013.

[27] Jeremy DW Clifton, Joshua D Baker, Crystal L Park, David B Yaden, Alicia BW Clifton, Paolo Terni, Jessica L Miller, Guang Zeng, Salvatore Giorgi, H Andrew Schwartz, et al. Primal world beliefs. *Psychological Assessment*, 31(1):82, 2019.

[28] Gerald L Clore, Norbert Schwarz, and Michael Conway. Affective causes and consequences of social information processing. In *Handbook of social cognition*, pages 323–418. Psychology Press, 2014.

[29] Colin D. Conrad, Jasmine R. Aziz, Jonathon M. Henneberry, and Aaron J. Newman. Do emotions influence safe browsing? toward an electroencephalography marker of affective responses to cybersecurity notifications. *Frontiers in Neuroscience*, 16:922960, 2022.

[30] W Alec Cram, Jeffrey G Proudfoot, and John D'Arcy. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, 31(4):521–549, 2021.

[31] Cynthia D. Fisher. *What do people feel and how should we measure it?* Bond University - School of Business Discussion Papers, 1997.

[32] Steve De Shazer, Yvonne Dolan, Harry Korman, Terry Trepper, Eric McCollum, and Insoo Kim Berg. *More than miracles: The state of the art of solution-focused brief therapy*. Routledge, 2021.

[33] Pieter Desmet. Measuring emotion: Development and application of an instrument to measure emotional responses to products. *Funology 2*, pages 391–404, 2018.

[34] Pieter Desmet, Peter Wassink, and Yancheng Du. Premo (emotion measurement instrument) card set: Male version, 2019.

[35] Marc Dupuis, Karen Renaud, and Anna Jennings. Fear might motivate secure password choices in the short term, but at what cost? In *Hawaii International Conference on System Sciences*, 2021.

[36] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2873–2882, 2015.

[37] Paul Ekman. Universals and cultural differences in facial expressions of emotion. In *Nebraska symposium on motivation*. University of Nebraska Press, 1971.

[38] Paul Ed Ekman and Richard J Davidson. *The nature of emotion: Fundamental questions.* Oxford University Press, 1994.

[39] Cori Faklaris, Laura A Dabbish, and Jason I Hong. A self-report measure of end-user security attitudes (sa-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 61–77, 2019.

[40] Leon Festinger and James M Carlsmith. Cognitive consequences of forced compliance. *The journal of abnormal and social psychology*, 58(2):203, 1959.

[41] Nico H. Frijda. Moods, emotion episodes, and emotions. In *Handbook of emotions*, pages 381–403. The Guilford Press, New York, NY, US, 1993.

[42] Nico H. Frijda, Peter Kuipers, and Elisabeth ter Schure. Relations among emotion, appraisal, and emotional action readiness. *Journal of Personality and Social Psychology*, 57(2):212–228, 1989.

[43] Nina Gerber and Karola Marky. The nerd factor: The potential of S&P adepts to serve as a social resource in the user's quest for more secure and Privacy-Preserving behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 57–76, Boston, MA, August 2022. USENIX Association.

[44] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? *Field Methods*, 18(1):59–82, 2006.

[45] Iwan Gulenko. Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security*, 22(2):167–178, 2014.

[46] Marco Gutfleisch, Markus Schöps, Stefan Albert Horstmann, Daniel Wichmann, and M Angela Sasse. Security champions without support: Results from a case study with owasp samm in a large-scale e-commerce enterprise. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 260–276, 2023.

[47] Julie M. Haney and Wayne G. Lutters. "it's Scary... It's Confusing... It's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security*, SOUPS 2018, pages 411–425, Baltimore, MD, August 2018. USENIX Association.

[48] Barbara Hewitt and Garry L White. Optimistic bias and exposure affect security incidents on home computer. *Journal of Computer Information Systems*, 62(1):50–60, 2022.

[49] Alice M Isen. *Toward understanding the role of affect in cognition.* Lawrence Erlbaum Associates Publishers, 1984.

[50] Daniel Kahneman. *Thinking, fast and slow*. macmillan, 2011.

[51] Elizabeth A Kensinger and Jaclyn H Ford. Retrieval of emotional events from memory. *Annual review of psychology*, 71:251–272, 2020.

[52] Stacey R Kessler, Shani Pindek, Gary Kleinman, Stephanie A Andel, and Paul E Spector. Information security climate and the assessment of information security risk among healthcare employees. *Health informatics journal*, 26(1):461–473, 2020.

[53] Saouré Kouamé and Feng Liu. Capturing emotions in qualitative strategic organization research. *Strategic Organization*, 19(1):97–112, 2021.

[54] Sara Kraemer and Pascale Carayon. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, 38(2):143–154, 2007.

[55] Ivar Krumpal. Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & quantity*, 47(4):2025–2047, 2013.

[56] Peter J Lang, Margaret M Bradley, and Bruce N Cuthbert. Emotion, attention, and the startle reflex. *Psychological review*, 97(3):377, 1990.

[57] Richard S. Lazarus. *Emotion and Adaptation*. Oxford University Press, 1991.

[58] Howard Leventhal. Findings and theory in the study of fear communications. *Advances in experimental social psychology*, 5:119–186, 1970.

[59] Huigang Liang, Yajiong Xue, Alain Pinsonneault, and Yu Andy Wu. What users do besides problem-focused coping when facing it security threats: An emotion-focused coping perspective. *MIS quarterly*, 43(2):373–394, 2019.

[60] Catherine A Lutz. *Unnatural emotions: Everyday sentiments on a Micronesian atoll and their challenge to Western theory*. University of Chicago Press, 2011.

[61] Heather McCosker, Alan Barnard, and Rod Gerber. Undertaking sensitive research: Issues and strategies for meeting the safety needs of all participants. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 2(1), 2001.

[62] Kevin Mclaughlin. *A Quantitative Study of Learner Choice in Cybersecurity Training: Do They Even Want Gamification?* PhD thesis, Colorado Technical University, 2023.

[63] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M Angela Sasse, and Imogen Verret. Why it security needs therapy. In *European Symposium on Research in Computer Security*, pages 335–356. Springer, 2021.

[64] NIST (National Institute of Standards and Technology). Framework for improving critical infrastructure cybersecurity, 2014.

[65] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different researchers, different results? analyzing the influence of researcher experience and data type during qualitative analysis of an interview and survey study on security advice. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–21, 2023.

[66] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security*, 66:40–51, 2017.

[67] Michael Quinn Patton. Qualitative research and evaluation methods. thousand oaks. *Cal.: Sage Publications*, 4, 2002.

[68] Michael Quinn Patton. Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*, 1(3):261–283, 2002.

[69] Reinhard Pekrun, Thomas Goetz, Wolfram Titz, and Raymond P Perry. Academic emotions in students' self-regulated learning and achievement: A program of qualitative and quantitative research. *Educational psychologist*, 37(2):91–105, 2002.

[70] Richard E Petty and Pablo Briñol. Emotion and persuasion: Cognitive and meta-cognitive processes impact attitudes. *Cognition and Emotion*, 29(1):1–26, 2015.

[71] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 1–18, Boston, MA, August 2022. USENIX Association.

[72] Michel Tuan Pham, Joel B Cohen, John W Pracejus, and G David Hughes. Affect monitoring and the primacy of feelings in judgment. *Journal of consumer research*, 28(2):167–188, 2001.

[73] Jonathan Posner, James A Russell, and Bradley S Peterson. The circumplex model of affect: An integrative approach to affective neuroscience, cognitive development, and psychopathology. *Development and psychopathology*, 17(3):715–734, 2005.

[74] Karen S Quigley, Kristen A Lindquist, and Lisa Feldman Barrett. Inducing and measuring emotion and affect: Tips, tricks, and secrets. *Handbook of research methods in social and personality psychology*, 220:252, 2014.

[75] Karen Renaud and Marc Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the new security paradigms workshop*, pages 42–56, 2019.

[76] Karen Renaud and Stephen Flowerday. Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications*, 34:76–81, 2017.

[77] Karen Renaud, Rosalind Searle, and Marc Dupuis. Shame in cyber security: effective behavior modification tool or counterproductive foil? In *New Security Paradigms Workshop*, pages 70–87, 2021.

[78] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):1–17, 2021.

[79] Hyeun-Suk Rhee, Young Ryu, and Cheong-Tag Kim. I am fine but you are not: Optimistic bias and illusion of control on information security. *ICIS 2005 proceedings*, page 32, 2005.

[80] Naomi B Rothman, Michael G Pratt, Laura Rees, and Timothy J Vogus. Understanding the dual nature of ambivalence: Why and when ambivalence leads to good and bad outcomes. *Academy of Management Annals*, 11(1):33–72, 2017.

[81] James A Russell. A circumplex model of affect. *Journal of personality and social psychology*, 39(6):1161, 1980.

[82] James A Russell and Lisa Feldman Barrett. Core affect, prototypical emotional episodes, and other things called emotion: dissecting the elephant. *Journal of personality and social psychology*, 76(5):805, 1999.

[83] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[84] Bruce Schneier. *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.

[85] Tali Sharot, Alison M Riccardi, Candace M Raio, and Elizabeth A Phelps. Neural mechanisms mediating optimism bias. *Nature*, 450(7166):102–105, 2007.

[86] Eric Shouse. Feeling, emotion, affect. *M/c journal*, 8(6), 2005.

[87] Matthias Vöhringer, Astrid Schütz, Sarah Gessler, and Michela Schröder-Abé. Sreis-d. *Diagnostica*, 66(3):200–210, 2020.

[88] Alexandra von Preuschen, Verena Zimmermann, and Monika C Schuhmacher. How do you feel about cybersecurity? - a literature review on emotions in cybersecurity. *Proceedings TecPsy 2023*, page 1, 2023.

[89] Xiaochen Angela Zhang and Jonathan Borden. How to communicate cyber-risk? an examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10):1336–1352, 2020.

[90] Verena Zimmermann and Karen Renaud. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131:169–187, 2019.

A Appendix: Data Analysis

Further supplementary material including an enlarged color version of the eye of cybersecurity-related emotions, an depiction of the causes (inner circle), analyses on mixed emotions and our codebook is available at: https://www.research-collection.ethz.ch/handle/20.500.11850/669758

	NEGATIVE																					POSITIVE									
	low-arousal															high-arousal							low-arousal					high-arousal				
	fearful	powerless	helpless	disappointed	annoyed	spiteful	uncomfortable	frustrated	averse	dismissive	dull	ashamed	bored	overwhelmed	impotent	indifferent	fatigued	left alone	dependent	insecure	tense	threatened	astonished	secure	happy	hopeful	trustful	calm	sympathetic	involved	action-motivated	empathetic	fascinated	interested
CAUSES																																	
Individual factors: Personal perceptions																																	
Level of Knowledge and Experience	•		•		•						•		•					•	•	•	•		•				•	•			•		•
Perceived Level of Protection (active)																							•	•	•		•						
Perceived Lack of Autonomy					•								•				•		•														
Internal Conflicts			•		•		•															•											
Perceived Vulnerability																•				•													
Anticipated Consequences	•	•	•																		•												
Perceived Value of Data																												•			•		•
Individual factors: Cybersecurity Perceptions																																	
Perceived Narrative and Relevance					•																•							•				•	•
Perceived Resource-Intensiveness and Hindrance					•			•			•				•	•												•					
Perceived Level of Control			•	•				•						•						•	•		•					•					
Perceived Level of Necessity					•														•	•	•							•					
Perceived Complexity													•																				
Media Reports as a Trigger for Cybersecurity Perceptions																					•												•
Interpersonal factors																																	
Self-perception and Perception of Others	•			•	•		•	•								•						•		•							•		
Level of Social Exchange					•			•										•					•										•
Perceived Relationship with Experts					•	•											•				•												
Organization-wide factors																																	
Perceived Level of Protection (passive)			•															•		•				•	•	•	•	•					
Perception of Design and Frequency of Education					•	•		•					•				•						•									•	•
Perceived Security Culture		•			•													•					•	•				•					
Perceived Demands and Requirements					•																												
Error Culture																																	
CONSEQUENCES																																	
Cognitive																																	
Psychological Distancing and Repression	•				•			•				•			•								•		•								
Externalization		•																								•	•	•					
Distorted concepts of cybersecurity and skills																							•										
Level of self-efficacy																							•										
Positive Outcome expectations																									•								
Behavioral																																	
Level of Attention, Awareness and Caution					•								•									•	•										•
Level and effectiveness of the approach to learning																•	•			•										•			
Avoidance and Rejection					•		•	•					•				•							•									
Knowledge-Behavior Gap					•		•					•											•		•								
Security-conscious Behavior																												•					
(Concealed) insecure Behavior	•																			•			•										•
Social																																	
Level of Social support seeking		•					•													•													•
Level of communality																	•	•												•	•		
Spillover																																	
Emotional exhaustion							•										•																
Reduced productivity					•																												
Need for recovery																																	

Table 1: Segment-wise analysis of causes and consequences and emotions (uniform emotions).

B Appendix: Interview

Interview Guideline

Introduction

- Participants were welcomed to the study and introduced to the background of the study
- Participants were reminded of participation conditions, acknowledging potential discomfort. They were encouraged to take time to answer, consider their responses, discontinue if necessary due to strong negative emotions, or seek further support afterward.
  - Spontaneously: When you think of cybersecurity, how does it make you feel?
  - How do you define cybersecurity?
- Interviewer provided a brief definition of the term cybersecurity

Emotions towards cybersecurity

1.a) General term of cybersecurity

- PrEmo was displayed. These questions were repeated until no further illustration showed the felt emotions:
  - Which of these illustrations best shows your feelings about cybersecurity?
  - What does this emotion mean to you?
  - How is this emotion expressed?
  - Can you scale this emotion from low to high on this scale?
  - Can you find a name for this emotion?
- The emotion word list was presented, and participants were instructed to mark feelings they experience, then narrow it down to three terms that best describe their feelings toward cybersecurity.
- Selected emotions were added to the main board. Questions on the understanding of the emotions are repeated if necessary
  - Please try to put yourself in a different position: How do you think your colleagues feel about cybersecurity in the workplace?

1.b Specific areas of cybersecurity

- Specific areas of cybersecurity were explained
  - I would like to ask you to tell me about your experience from your everyday work in relation to these aspects. Share what comes to mind, take as much time as you need, and please focus on how you felt in these situations. I will not interrupt you for now, but I will be making notes on the side.

Top Emotions

- Participants could add further emotions to the main board if wished
- Three emotions (top emotions) were selected for the further interviewing process

Antecedents

- The following questions were asked:
  - Why do you feel the way you do when you think about cybersecurity (Top 3)?
  - What emotion would you like to feel towards cybersecurity?
  - Assuming a miracle happens overnight, and you feel (emotion from question before) towards cybersecurity - What would change?
  - What would have happened for you to now feel this emotion?
  - What emotion would you prefer not to feel towards cybersecurity?
  - What would have happened for you to now feel this emotion?

Consequences

- The following questions were asked:
  - Do these emotions have an impact on your behavior (Top emotions) towards cybersecurity? How?
  - How do your emotions towards cybersecurity influence your daily work/primary tasks?

Coping

- The following questions were asked:
  - Is there something that helps you deal with these emotions? What?
  - Is there something your company/employer can do to address these emotions? What?

Self-efficacy

- A scale was displayed in miro
  - How confident are you in your ability to engage with cybersecurity in general (e.g., learning cybersecurity content or implementing company guidelines)?
  - Why is that the case?

Interview Demographics

Participant	Age	Gender	Industry	Work experience (years)	Interview duration
P1	20 - 24	f	Research and education	1 - 5	0:45
P2	20 - 24	f	Research and education	1 - 5	0:40
P3	20 - 24	f	Marketing	1 - 5	0:43
P4	25 - 29	f	Finance	1 - 5	0:46
P5	20 - 24	m	Engineering	1 - 5	0:43
P6	50 - 54	m	Pharmaceuticals	21 - 25	0:42
P7	60 - 64	m	Engineering	36 - 40	1:07
P8	20 - 24	f	Research and education	1 - 5	0:24
P9	50 - 54	f	Healthcare	16 - 20	0:30
P10	20 - 24	m	Research and education	1 - 5	0:32
P11	20 - 24	f	Healthcare	1 - 5	0:30
P12	55 - 59	m	Information technology	31 - 35	0:35
P13	30 - 34	m	Consulting	11 - 15	0:40
P14	18 - 19	m	Healthcare	1 - 5	1:15
P15	25 - 29	m	Consulting	1 - 5	1:15
P16	35 - 39	m	Insurance	16 - 20	1:04
P17	45 - 49	m	Research and Education	16 - 20	1:19
P18	30 - 34	m	Public sector	6 - 10	1:12
P19	45 - 49	m	Information technology	21 - 25	0:48
P20	50 - 54	f	Administration	31 - 35	1:08
P21	25 - 29	f	Consulting	6 - 10	0:54
P22	55 -59	f	Research and education	21 - 25	1:27
P23	30 - 34	m	Administration	11 - 15	1:15
P24	30 - 34	m	Engineering	6 - 10	0:53
P25	35 - 39	m	Engineering	6 - 10	0:55
P26	25 - 29	f	Pet sector	1 - 5	0:53

Table 2: Participant demographics. For privacy, department and rank are omitted; industries, age and work experience categorized

Scale	Variable	M	SD	MIN	MAX	MEDIAN
SREIS	Perceiving Emotion	3.77	0.48	2.75	5.00	3.75
SREIS	Use of Emotion	3.10	0.75	1.00	4.33	3.00
SREIS	Understanding Emotion	3.23	0.72	2.00	5.00	3.25
SREIS	Managing Emotion (self)	3.46	0.71	2.00	4.75	3.50
SREIS	Social Management	3.68	0.59	2.50	4.75	3.75
SREIS	Emotional Intelligence Score	3.45	0.36	2.87	4.30	3.41
HAIS-Q	Knowledge_Password management	4.71	0.43	3.67	5.00	5.00
HAIS-Q	Knowledge_Email Use	4.26	0.62	2.67	5.00	4.33
HAIS-Q	Knowledge_Internet use	4.47	0.65	2.67	5.00	4.67
HAIS-Q	Attitude_Password management	4.71	0.40	3.33	5.00	4.83
HAIS-Q	Attitude_Email Use	4.56	0.43	3.67	5.00	4.67
HAIS-Q	Attitude_Internet use	4.63	0.43	3.67	5.00	4.67
HAIS-Q	Behavior_Password management	4.68	0.41	3.67	5.00	5.00
HAIS-Q	Behavior_Email Use	4.40	0.65	3.00	5.00	4.67
HAIS-Q	Behavior_Internet use	3.90	0.78	2.67	5.00	3.83
HAIS-Q	SUM_Password management	14.09	0.95	11.33	15.00	14.33
HAIS-Q	SUM_Email Use	13.22	1.45	9.67	15.00	13.33
HAIS-Q	SUM_Internet use	13.00	1.57	9.67	15.00	13.33
ISCI	ISCI_Practices	6.69	2.57	3.00	12.00	6.00
ISCI	ISCI_Importance	12.54	2.16	8.00	15.00	12.50
ISCI	ISCI_Laxness	5.04	1.97	3.00	9.00	4.50
ISCI	ISCI_Score	10.73	1.41	7.67	13.67	10.67

Table 3: Screening. Controls and variables to maximize variation. EI was measured to ensure emotions reflection skills. We retained all participants to preserve diversity and avoid bias, monitoring those with slightly noticeable scores without issues.

C Appendix: Qualitative Survey

Qualitative Survey: Method

Welcome. Participants were provided information on the study's conditions, procedure, and purpose, including background details on participant rights and data processing, and granted consent upon agreement with the outlined conditions.

Emotional Cybersecurity Events, Emotions towards Cybersecurity and Consequences.

- When you think about cybersecurity at work, what emotions do you feel?
- Put yourself in these emotions. Why do you feel these emotions towards cybersecurity at the workplace? Are there specific events that led to these emotions?
- What was the result of these emotions? e.g. Do your feelings affect your security behavior or the way you approach your work? How does this affect your attitude toward work?

Thoughts on cybersecurity. Based on Renaud et al., participants were asked to describe their spontaneous thoughts about cybersecurity in open questions and to record what was unsaid [78].

- What are the first thoughts that come to mind when you hear the term of 'cybersecurity'?
- What have you always wanted to say about cybersecurity?

Cybersecurity definition and behavior. A brief definition of cybersecurity was introduced, and participants were asked to name behaviors they feel are necessary to protect cyberspace within organizations. Separately, participants were asked which measures they actually implement.

- What should you do to protect yourself against cyber attacks at the workplace?
- What measures do you actually take to protect yourself against cyber attacks at the work place?

Cybersecurity Incident Experience. Participants who could not name any experiences were allowed to skip the item.

- Have you ever been the victim of a cyber attack? Please describe your experience as detailed as possible. Place emphasis on your emotional journey throughout the experience.

Closing. Cybersecurity-specific, organization-specific and general demographic data was collected. To collect security-specific data, the Security behavior intentions scale (SeBIS; [36]) for the collection of behavioral intentions and the SA-6 for the collection of security attitudes [39]. In addition, information on gender, age, education, employment status , industry and company size were provided.

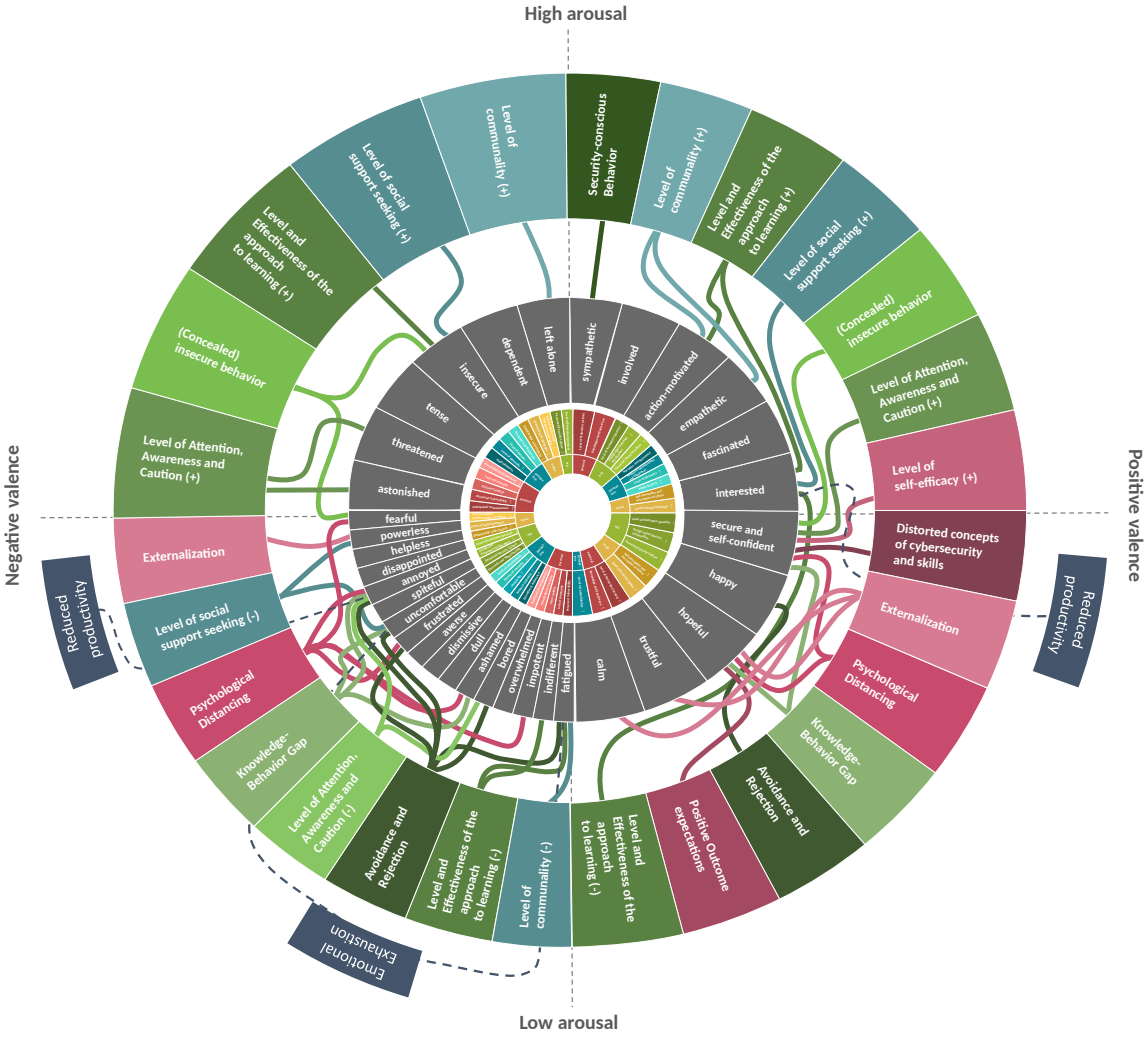
Qualitative Survey Demographics

Scale	Variable	*M*	*SD*
SeBis	Device Securement	4.39955357	0.66602819
SeBis	Password Generation	3.70758929	0.88065037
SeBis	Protective Awareness	3.9	0.87423436
SeBis	Updating	3.5922619	0.91689372
SA-6	Score	3.44494048	0.96192092
Age Group			
< 19		1	
20 -24		29	
25 - 29		22	
30 - 34		9	
35 - 39		11	
40 - 44		9	
45 - 49		5	
50 - 54		9	
55 - 59		14	
60 - 64		2	
Gender			
female		32	
male		78	
non-binary		2	
Company Size			
1-9		10	
10-49		18	
50-249		14	
250-1000		15	
>1000		54	
Industry			
Chemistry & Raw Materials		3	
Agriculture		1	
Construction		4	
Services & Crafts		3	
Energy & Environment		2	
Finance, Insurance & Real Estate		26	
Commerce		2	
Internet		4	
Consumption		1	
Media		4	
Metallurgy & Electronics		2	
Pharmaceuticals & Health		9	
Education		6	
Technology & Telecommunications		7	
Tourism & Hospitality		1	
Transportation & Logistics		2	
Economy & Politics		7	
Other		28	

Table 4: Participant demographics. Quantitative measurements were included to add further depth to the understanding of the sample and ensure a diverse representation across selected variables.

Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity: Digital Appendix

A Eye of cybersecurity-related emotions



See C for a larger depiction of the causes.

B Interview: Emotion List

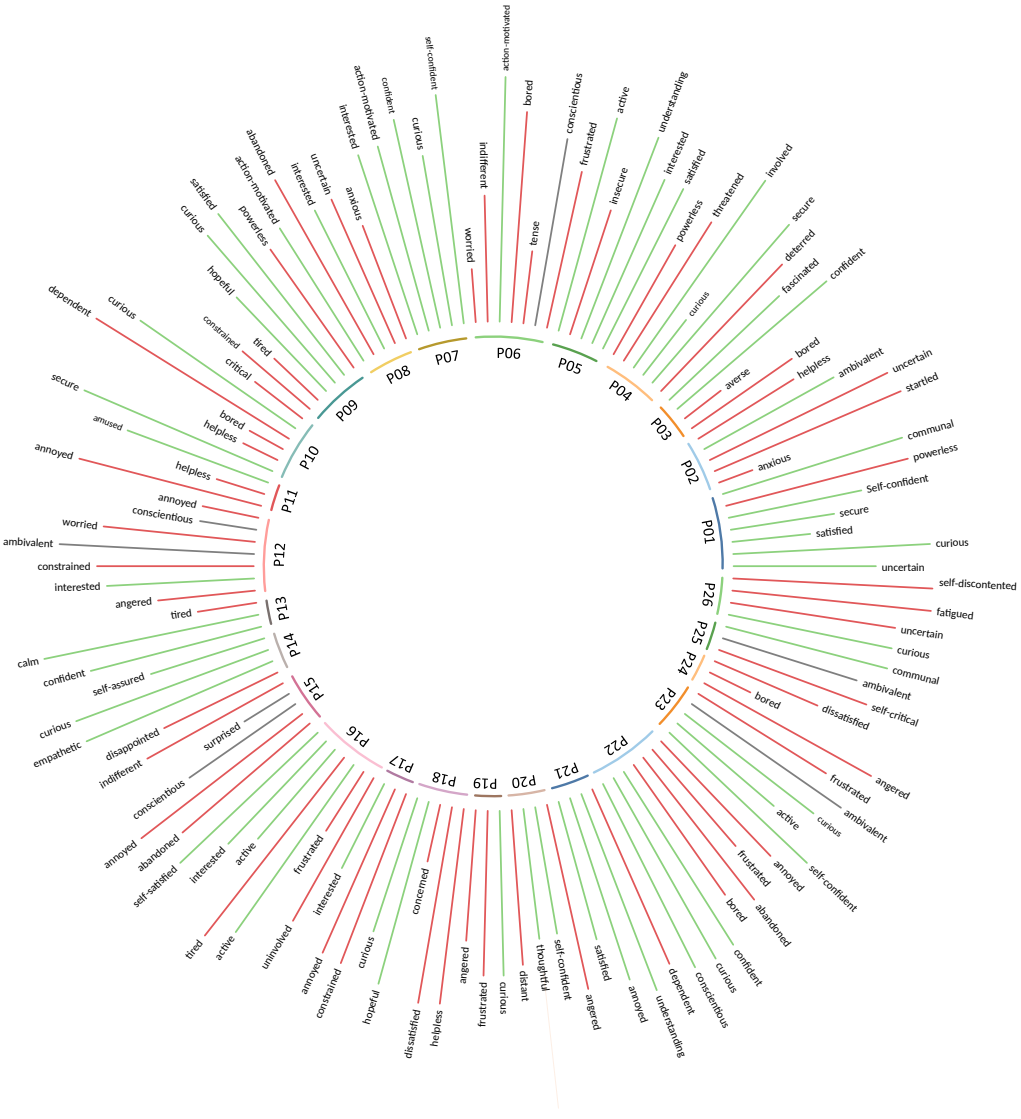
Valence	Emotion	Source
positive	active, satisfied, enthusiastic, grateful, passionate, enthusiastic, relaxed, enlightened, fascinated, cheerful, glad, secure, calm, happy, thrilled, hopeful, in the flow, Inspired, interested, involved, love, curious, optimistic, secure, proud, enjoyment, relief, trust, satisfied, confident	[2, 6–8, 11, 12]
negative	neglect, dependent, loneliness, tense, anxious, dread, despair, ashamed, insult, worried, narrowly, intimidated, dispirited, disappointed, humiliated, frustrated, bored, annoyed, nervous, helpless, dull, guilty, disappointed, sad, stunned, insecure, dissatisfied, annoyed, confused, furious	[1–7, 9, 10, 12, 14]
neutral	ambivalent, indifferent, surprised, independent, unconcerned	[4, 7, 12, 13]

Emotion list for the help of verbalizing emotions during the interviews. Emotions were selected from consisting emotion research in cybersecurity or similar (application) areas such as academic learning, emotions towards IT usage or emotions at the workplace in general

C Overview of causes for cybersecurity emotions

Note: Arrow up = Level rather high; more positive than negative statements; Arrow down = Level rather low; more negative than positive statements; no arrow = no clear direction; not level but change in characteristic e.g. narrative of cybersecurity; Please refer to table 1 within the paper for connections to the investigated emotions

D Intensity ratings across named emotions



Emotions displayed per participant.

E Document-wise analysis of causes, consequences and emotions

	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26
CAUSES																										
Within-person factors: Personal perceptions																										
Level of knowledge and experience	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Perceived Level of Protection (active)	•	•		•	•		•		•		•		•	•		•				•		•	•	•		•
Perceived Lack of autonomy	•					•			•	•	•	•	•			•	•	•		•	•			•		•
Internal Conflicts		•	•										•	•	•			•	•	•	•		•		•	
Perceived vulnerability				•			•			•	•		•	•		•				•	•		•		•	
Anticipated Consequences	•	•		•	•			•	•					•							•	•				•
Perceived value of data				•	•		•						•										•		•	
Within-person factors: Cybersecurity Perceptions																										
Perceived Narrative and Relevance																										
Perceived Resource-Intensiveness and Hindrance				•	•	•			•	•			•		•	•	•	•	•	•	•	•		•		•
Perceived Level of control	•			•					•		•	•	•			•		•		•		•	•			
Perceived Level of Necessity				•	•	•					•	•		•	•		•		•	•	•			•	•	•
Perceived Complexity									•		•			•	•										•	•
Media reports as a trigger for cybersecurity perceptions		•					•				•			•		•		•				•				•
Interpersonal factors																										
Self-perception and perception of others		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•
Level of Social Exchange		•					•	•	•			•		•	•		•	•		•	•		•	•	•	•
Perceived Relationship with Experts					•		•			•	•		•	•	•	•	•	•		•	•		•	•		•
Organization-wide factors																										
Perceived Level of Protection (passive)	•	•	•	•	•	•	•	•	•	•		•	•		•				•		•	•	•	•	•	•
Perception of Design and Frequency of Education			•	•		•	•		•		•	•	•	•	•	•	•	•	•	•		•		•		•
Perceived Security Culture	•			•	•	•	•			•	•		•		•	•		•	•		•	•	•	•		
Perceived Demands and Requirements			•	•		•		•		•	•	•		•	•		•			•	•			•	•	•
Error Culture				•	•				•					•	•	•					•	•			•	•
EMOTIONS																										
high-arousal, positive valence	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•		•	•
low-arousal, positive valence	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	
high-arousal, negative valence	•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•	•	•
low-arousal, negative valence	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
CONSEQUENCES																										
Cognitive																										
Psychological Distancing and Repression	•	•	•	•					•		•	•	•				•	•		•	•	•		•		•
Externalization		•	•	•			•		•		•	•			•	•				•				•		•
Distorted concepts of cybersecurity and skills		•		•	•	•				•	•	•					•			•	•					
Level of self-efficacy	•			•		•	•				•		•			•		•						•		
Positive Outcome expectations	•	•				•			•									•							•	
Behavioral consequnces																										
Level of Attention, Awareness and Caution																										
Level and effectiveness of the approach to learning	•	•		•		•		•		•				•	•		•	•	•		•					•
Avoidance and Rejection		•	•	•		•		•	•					•	•					•	•	•		•		•
Knowledge-Behavior Gap		•	•						•	•		•			•		•	•		•	•				•	•
Security-conscious Behavior	•					•	•			•		•			•		•				•	•			•	
Concealed insecure and insecure Behavior		•								•	•										•	•			•	
Social consequnces																										
Level of Social support seeking																										
Level of communality							•						•	•			•	•	•				•		•	
Spillover consequences																										
Emotional exhaustion	•	•			•				•	•	•		•	•	•		•	•				•	•	•		•
Reduced productivity			•			•			•		•	•						•	•		•			•		•
Need for recovery						•								•					•		•	•	•	•		

F Codebook

Theme	Subthemes	Code Index (#)	Example
			CAUSES
Individual factors: Personal perceptions	Level of knowledge and experience	1	"I feel insecure because I am unable to recognise, assess and evaluate the dangers and safety measures myself due to a lack of knowledge. (S_P91)"
		2	"[...] because I don't know what and how I can implement it [cybersecurity] or what exactly the consequences are of such an attack or something like that (I_P02)"
		3	"I'm a bit scared and insecure about the subject because, as I said, I don't know that much about it, but I know that a lot of bad things can happen (I_P08)"
		4	"I have no idea what to do in case I get hacked or something (I_P10)."
		5	"I simply think that I would be much more likely to do something if a mistake were made. (I_P01)"
		6	"Because I've been working with computers for about 40 years, and because I've already dealt with many passwords and various things. (I_P11)"
		7	"Your interest in cybersecurity is not just in the workplace, but also in the data protection of your own data (I_P07)"
		8	"I am usually annoyed in that case when I am just establishing a new thing. (I_P15)"
		9	"I've also received spam emails in my private life, which I successfully identified as such and deleted. And that gave me a bit of a sense of achievement that I didn't fall for it. (I_P02)"
	Perceived Level of Protection (active)	10	"because, let's say subjectively, I would say that yes, I also have it quite well under control. There is no urgent need for action now. (I_P09)"
	Perceived Lack of autonomy	11	"I get a kick out of recognizing things myself and not going along with things, because I generally always reject coercion (I_P11)"
		12	"So I don't have any freedom of choice, I'm just dependent on the arbitrary order to do it that way. (I_P21)"
	Internal Conflicts	13	"It's a narrative that cybersecurity is an insecure restriction of personal rights. (I_P17)"
		14	"But I realize that's just the way it is in today's world. You have to be vigilant, you have to be attentive and you have to learn to deal with it. So that's the way it is, I accept it now, I accept it for myself, even though I don't always like it. (I_P21)"
	Perceived vulnerability	15	"I'm too uninteresting, so I'm not interested. (I_P16)"
		16	"When I think about it, it was like "Oh well, oh well, it's probably all coincidence, we've probably got it really well under control". (I_P25)"
	Anticipated Consequences	17	"It's always presented as if it's really bad and everything is so negative and that it somehow has far-reaching consequences for us as humanity and so on. (I_P02)"
		18	"That's why some employees, or perhaps even myself, are not even aware of the dangers. (I_P05)"
		19	"And if you don't pay attention to the fact that something can happen quickly and you yourself will of course get into trouble as well (I_P04)"
	Perceived value of data	20	"Because the data you work with must not be passed on to others, they are very worthy of protection. (I_P07)"
Individual factors: Cybersecurity Perceptions	Perceived Narrative and Relevance	21	"I just think it's so present now. Everywhere (I_P07)."
		22	"On the one hand, I would just be so disinterested when it comes to cybersecurity, but I find that, then again I'm interested in how something like that takes place when it comes to things like that, how hackers go about it, so to speak. (I_P03)"
	Perceived Resource-Intensiveness and Hindrance	23	"There is simply the amount of work involved and the inconvenience outweighs this (I_P17)"
		24	"When I wanted to do things quickly online and was held up by cybersecurity measures that I didn't understand and I couldn't resolve my issue quickly (S_P7)"

Theme	Subthemes	Code Index (#)	Example
	Perceived Level of control	25	"Powerlessness, especially with regard to things that are not in my control. So the things that are in my power, so to speak. So as I said earlier, these hacker attacks or things like that (I_P01)"
		26	"However, I don't feel that I can do that much about cyber attacks myself and am exposed to the whole thing (S_P01)"
		27	"Well, I can't do that. As I said, I'm not an IT professional. (I_P20)"
		28	"I don't know how many employees we have and yes, my influence is relatively small, I would say. (I_P18)"
	Perceived Level of Necessity	29	"You are dependent on cybersecurity. It is a necessary evil (I_P24)"
		30	"It's annoying but necessary. (S_P92)"
	Perceived Complexity	31	"It's such a complex topic that you can't know everything. (I_P25)"
	Media reports as a trigger for cybersecurity perceptions	32	"It's always portrayed as if it's really bad and everything is so negative and that it somehow has far-reaching consequences for us as humanity and so on. (I_P02)"
Interpersonal factors	Self-perception and perception of others	33	"I am actually concerned sometimes. How? How naive or how narrow-minded my environment reacts to one thing or another. (P14)"
		34	"When I hear the word cybersecurity, the first thing that comes to mind is naivety and stupidity. On further reflection, I also think of ignorance and carelessness. (S_P69)"
		35	"It's still kind of a man's thing. (I_P18)"
		36	"Sometimes I'm embarrassed about myself, in the sense of what kind of background [IT background] I actually have, whether others know that. How others think about me and I don't think that [cybersecurity] is important to them either and sometimes they don't care. But there are times when I get a bit annoyed with myself and even think to myself, you could actually do better. You actually know what you can do better. (I_P25)"
		37	"Maybe I just don't want to describe myself as paranoid. (I_P18)"
		38	"They were born into it. I think some fields are still new to me. But I see it in my use of the cell phone. I have to ovecome an inhibition threshold before I try something (I_P21)"
		39	"And the others are all 50 plus. And when they come to me and ask me how it works or how to set up a VPN and I have to tell them, I'd say that's a bit of an ego boost. (I_P06)"
	Level of Social Exchange	40	"Never talked about it, never had the feeling that there was a mood. (I_P20)"
	Perceived Relationship with Experts	41	"But, knock on wood, I haven't had any contact with them yet (I_P05)"
		42	"Sometimes you really are treated like a small child who just doesn't know how the internet works yet. (I_P10)"
		43	"I think that's more like bullying. (I_P11)"
Organizational factors	Perceived Level of Protection (passive)	44	"Simply because I feel secure. In other words, I have a sense of security and am therefore confident that the mechanisms that have already been implemented will work, and at the same time there are specialists, archiving experts or representatives who deal with the issues and derive how we can implement and improve this in our company (I_P07)"
		45	"I don't need to be afraid that someone has access to my data. That wouldn't be possible without cybersecurity. (S_P78)"
	Perception of Design and Frequency of Education	46	" I'm annoyed because I assume that some things don't need to be told to us ten times, we know them. (I_P11)"
		47	"Cybersecurity training targets the lowest hanging fruit, like clicking links on phishing emails. There's never details about the latest more sophisticated attacks, we're always training to the lowest common denominator. (S_P88)"
	Perceived Security Culture	48	"That's a bit critical of our employer's management as there are also a lot of issues when it comes to getting a job done. So there are already gray areas being entered in order to get it done. Then it doesn't really matter at that moment. Be it that we break data protection regulations. (I_P22)"
		49	"I find it simply unbelievable how naively and carelessly companies and their management deal with cybersecurity. (S_P69)"
	Perceived Demands and Requirements	50	"Some things that are imposed by IT, security or cybersecurity are simply not practicable to implement in working life or in normal life without creating major hurdles. (I_P24)"
	Error Culture	51	"But how am I supposed to learn from mistakes if I'm not told about them? (I_P14)"

Theme	Subthemes	Code Index (#)	Example
			CONSEQUENCES
Cognitive	Psychological Distancing and Repression	52	"My thought was not to let something get to you in such a way that you don't drive yourself crazy. (I_P20)"
	Externalization	53	"Overall, I basically rely on the people who work in the departments, in compliance as data protection officers or information protection officers, to carry out their work in this area so conscientiously that they protect the entire company. (I_P07)"
		54	"I rely on my employer to protect his company. (S_P85)"
	Distorted concepts of cybersecurity and skills	55	"The [colleague] says " Is it really that secure?" This password is so simple, I always have such a short one, at least I can remember it. I'm already trying to dice more with letters, special characters, upper and lower case, numbers. So now I actually have more than four characters. (...) It's working and it's all great. (...) It's the ideal situation. (I_P20)"
	Level of self-efficacy	56	"My confidence in my ability to deal with server security is relatively high. I attribute this to my solid understanding of how these systems work (I_P13)."
	Positive Outcome expectations	57	"You know it's somehow not ideal and hope that nothing will go wrong anyway. (I_P18)"
Behavioral	Level of Attention, Awareness and Caution	58	"I try to be careful. There are certainly many more things you can do and I don't want to be arrogant about it, but I try to be careful. (I_P11)"
	Level and effectiveness of the approach to learning	59	"I think if there was something new now, maybe boredom would prevent me from relearning it, or at least slow me down. (I_P06)"
	Avoidance and Rejection	60	"[This leads to] me not wanting to deal with the issue. And generally not wanting to have anything to do with it at work if I don't have to. (I_P03)"
	Knowledge-Behavior Gap	61	"We have instructions for that too. I know what these passwords should look like. But yes, I can only say to myself that I usually use a password that I can remember well. And that's just it. Rather the simple ones, yes. Not the super secure ones, I'll admit that. (I_P12)"
	Security-conscious Behavior	62	"I paid more attention, because it's not just about me, that I came up with more creative passwords and that I'm extra sure that my VPN is working now (I_P06)"
		63	"I am focussing on even stronger passwords (and if possible, the use of 2-factor authentication) (S_P37)"
	(Concealed) insecure Behavior	64	"I have my file where I write it down. I know they are also saved on the computer. Under passwords. Yes, I don't have them all saved in my head. I'll have to look them up (I_P21)"
Social	Level of Social support seeking	65	"When I'm really angry, I can also vent my anger in our office. Then I always get approval. If you're angry, you're not angry alone. Or I have someone I can discuss it with. And then I'm doing quite well (I_P16)"
		66	"Nowadays, when I say IT or cybersecurity, it has a negative connotation. And that's why I try to avoid the term in order to avoid the feeling. (I_P14)"
	Level of communality	67	"Proactively confronting it [attacks] with an open eye and then also taking measures, for example by writing to the team. "We currently have phishing emails. Someone is pretending to be someone else" (I_P07)"
Spillover	Emotional exhaustion	68	"Sooner or later, it ensures that if this emotion were permanent. It turns into a kind of aversion and therefore the measures are not implemented, which leads to scenario two in the long term. (I_P15)"
		69	"Because I see fear as limiting me rather than somehow continuing (I_P22)"
		70	"Life [without cybersecurity] would be easier, there would be less stress and certainly less burnout at work. (I_P14)"
		71	"Of course, I'm also angry at my employer for constantly making life difficult for me. (I_P13)"
	Reduced productivity	72	"Maybe that would make me less effective that day. (I_P06)"
		73	"If I'm not expecting an email, then I don't pay attention to the emails. I'm actually quite strict about that. And if someone really has something important, they can either send me another email or call me. (I_P12)"
	Need for recovery	74	"This of course has a very drastic effect on the whole thing. That's when we actually reach the point where we simply say that we won't use it at all or, in case of doubt, we won't continue with our work. Simply standstill. (I_P24)"

References

[1] Eric Bachura, Rohit Valecha, Rui Chen, and H Raghav Rao. The opm data breach: An investigation of shared emotional reactions on twitter. *MIS Quarterly*, 46(2), 2022.

[2] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4):1228–1247, 2019.

[3] W Alec Cram, Jeffrey G Proudfoot, and John D'Arcy. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, 31(4):521–549, 2021.

[4] Cynthia D. Fisher. *What do people feel and how should we measure it?* Bond University - School of Business Discussion Papers, 1997.

[5] Robin H Kay and Sharon Loverock. Assessing emotions related to learning new software: The computer emotion scale. *Computers in Human Behavior*, 24(4):1605–1623, 2008.

[6] Barry Kort, Rob Reilly, and Rosalind W Picard. An affective model of interplay between emotions and learning: Reengineering educational pedagogy-building a learning companion. In *Proceedings IEEE international conference on advanced learning technologies*, pages 43–46. IEEE, 2001.

[7] Alessandro Murgia, Parastou Tourani, Bram Adams, and Marco Ortu. Do developers feel emotions? an exploratory analysis of emotions in software artifacts. In *Proceedings of the 11th working conference on mining software repositories*, pages 262–271, 2014.

[8] Reinhard Pekrun, Thomas Goetz, Wolfram Titz, and Raymond P Perry. Academic emotions in students' self-regulated learning and achievement: A program of qualitative and quantitative research. *Educational psychologist*, 37(2):91–105, 2002.

[9] Reinhard Pekrun and Elizabeth J. Stephens. Academic emotions. In *APA educational psychology handbook, Vol 2: Individual differences and cultural and contextual factors*, APA handbooks in psychology, pages 3–31. American Psychological Association, Washington, DC, US, 2012.

[10] Karen Renaud, Rosalind Searle, and Marc Dupuis. Shame in cyber security: effective behavior modification tool or counterproductive foil? In *New Security Paradigms Workshop*, pages 70–87, 2021.

[11] Bret L Simmons, Janaki Gooty, Debra L Nelson, and Laura M Little. Secure attachment: Implications for hope, trust, burnout, and performance. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, 30(2):233–247, 2009.

[12] Charles Richard Snyder and Shane J Lopez. *Handbook of positive psychology*. Oxford university press, 2001.

[13] Mari-Klara Stein, Sue Newell, Erica L Wagner, and Robert D Galliers. Coping with information technology. *Mis Quarterly*, 39(2):367–392, 2015.

[14] Xiaochen Angela Zhang and Jonathan Borden. How to communicate cyber-risk? an examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10):1336–1352, 2020.

Chapter 4

Paper B: Improving Emotions Towards Cybersecurity

The paper was published as follows:

Nina Gerber, Verena Zimmermann, Alexandra von Preuschen, and Karen Renaud. 2025. Unpacking the social and emotional dimensions of security and privacy user engagement. In Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025). USENIX Association, Seattle. 535-554. https://www.usenix.org/conference/soups2025/presentation/gerber

Unpacking the Social and Emotional Dimensions of Security and Privacy User Engagement

Nina Gerber*
Technical University of Darmstadt

Verena Zimmermann*
ETH Zurich

Alexandra von Preuschen
Justus-Liebig-University Gießen

Karen Renaud
University of Strathclyde, UK
University of South Africa, South Africa
Rhodes University, South Africa

Abstract

Despite the acknowledged importance of security and privacy (S&P), user engagement with protective practices remains limited, influenced by complex social dynamics and emotional responses. In this study, we surveyed a representative sample of 496 U.S. participants to examine the interplay between social dynamics and emotional responses in shaping S&P behaviours. Our findings highlight that S&P conversations are infrequent, hindered by perceived social norms, complexity, and assumed disinterest from others. Participants associated S&P-savvy individuals with positive traits such as trustworthiness and intelligence, yet also challenge stereotypes of paranoia or social awkwardness. Normalizing discussions and fostering social interactions around S&P could drive greater user engagement. Emotionally, S&P practices evoke not only frustration, fear, and feelings of being overwhelmed, but also curiosity and a desire for empowerment. Participants cited simplification, enhanced self-efficacy, and tangible evidence of the impact of their actions as critical factors making S&P more approachable and engaging. These insights suggest opportunities to design socially supportive and emotionally resonant interventions to improve user adoption of S&P behaviours.

1 Introduction

In today's complex, digitised and interconnected world, security and privacy (S&P) are crucial [17, 59]. However, despite their importance, many users struggle to adopt S&P protection measures. These challenges stem from various barriers, including a lack of awareness and skills, misconceptions about the efficacy of such measures, or simply a lack of motivation [21, 41, 42, 57, 71]. In recent years, the understanding of S&P as a social phenomenon [46, 52, 82] and the impact of emotional and psychological factors on users' engagement with S&P has gained attention. These factors were found to be closely intertwined [77] and suggest promising directions in predicting S&P behaviours [2, 29, 77].

Prior studies have shown that security is often associated with negative emotions such as fear, frustration, and uncertainty, which can hinder users' adoption of protective behaviours [42, 65, 77]. For instance, users frequently describe S&P measures as overwhelming, with the domain often perceived as *mystical, unknown, and fearful* to non-experts [19, p.1]. In contrast, positive emotional responses with high arousals, such as interest, were found to foster protective behaviours [77].

Despite extensive efforts to improve the usability of S&P measures, little attention has been given to fostering positive emotional engagement with S&P. Shifting from fear-driven narratives to a focus on enjoyment and empowerment could open new avenues for enhancing user engagement. This motivates our first research question:

RQ1: How can S&P be made more enjoyable, and what positive attributes do users associate with S&P? *This question seeks to uncover the factors driving both positive and negative emotional responses to S&P. We aim to identify strategies that make S&P more engaging and identify the positive and negative attributes users associate with S&P, aiming to uncover opportunities to enhance the broader perception of S&P.*

Social dynamics and emotions are found to be closely interconnected, with social dynamics causing emotional responses, and vice versa [77]. They have shown promise in addressing barriers to S&P adoption, such as raising awareness of S&P issues through informal storytelling [58, 61], or prompting actions like software updates and privacy settings

*Both authors contributed equally to this work.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

adjustments [20]. Social cues also help users navigate S&P settings more effectively [23, 24, 28]. However, S&P topics remain under-discussed among non-expert users [22, 77], and experts often hesitate to engage in these conversations with non-experts due to fears of disinterest or negative reactions [35].

To leverage the full potential of social dynamics for improving S&P practices, it is essential to understand why people choose to engage in or to avoid conversations about S&P and identify strategies to encourage these discussions. This leads to our second research question:

RQ2: What facilitates social interactions on S&P? *We aim to explore the barriers and enablers of S&P discussions, how frequently people talk about S&P topics, identify opportunities for fostering such conversations, and examine how stereotypes surrounding S&P might influence social interactions.*

By addressing these research questions, our study aims to provide actionable insights into the emotional and social dynamics of S&P, contributing to improved user engagement and reshaping the broader perception of S&P practices.

We conducted a survey study with a representative sample of 496 U.S. participants, combining quantitative Likert-scale ratings and qualitative open-ended questions. Our findings reveal that while S&P is widely recognised as important and predominantly associated with positive traits such as trustworthiness and reliability, security may invoke negative affect with participants feeling overwhelmed and fearful due to perceived knowledge gaps, leading to disengagement. They highlighted the need to enhance knowledge, accessibility, and self-efficacy to make S&P practices more engaging and enjoyable. Privacy, in contrast, was frequently described as a controversial and sensitive topic, which is sometimes perceived as hypocritical and overly complicated. Participants expressed a desire for greater societal attention to S&P, advocating for more frequent discussions.

Still, conversations about S&P topics remain rare, hindered by assumed disinterest of peers and social taboos. Participants suggested that external triggers, such as increased media coverage or organisational training, could encourage more S&P-related dialogue. Fear of being stereotyped might also influence willingness to discuss S&P topics: While S&P-conscious people are typically associated with positive attributes like intelligence, certain privacy practices, such as avoiding social media or using encryption, are sometimes labelled as paranoid. These findings highlight the need for interventions that address both the emotional barriers and social dynamics surrounding S&P to foster better engagement and discourse.

This research supports stakeholders that shape usable S&P practices, including researchers, practitioners responsible for security awareness (e.g., CISOs, privacy and security champions, and leadership roles), and system and software designers who seek to create more positive, socially grounded user interactions through the following contributions:

- Our findings extend the understanding of emotional responses towards S&P. Although S&P are predominantly associated with positive traits such as trustworthiness and reliability, security often evokes negative emotions such as fear and overwhelm, driven by perceived knowledge gaps. Privacy, in contrast, is viewed as controversial and sometimes hypocritical, highlighting a nuanced perception of these domains. These findings add to our understanding of user disengagement and suggest pathways for improving accessibility and user experiences in S&P.

- We identify key social and psychological factors that inhibit S&P discussions, including assumed disinterest of others and social taboos. Interestingly, the participants appeared to overestimate the effectiveness of their own S&P measures, as compared to those of colleagues, acquaintances, and especially parents, while underestimating others' willingness to discuss S&P-related topics. Thus, enhancing communication, e.g., through triggering S&P conversations similar to the social triggers described by Das et al. [20], might not only help in organisational but also in private settings, to overcome negative S&P-related perceptions, increase engagement, and better align users' self-appraisals with the actual effectiveness of S&P measures and behaviours.

- Our results highlight the dual-edged nature of S&P stereotypes, where S&P-conscious individuals are admired for their intelligence but also risk being perceived as paranoid. These insights underline the need for strategies to normalise and facilitate S&P discourse in social and professional contexts to counter such stereotypes.

2 Related Work

To set the scene, we summarise related work covering emotional and social dimensions of S&P. We conclude with the implications for our study.

2.1 S&P-related Emotions & Perceptions

As participants in prior research faced challenges in clearly identifying emotions [77], often confusing them with similar constructs, we adopt a broader interpretation of the term, which includes both perceptions and emotions.

The American Psychological Association (APA) defines perceptions as *the process or result of becoming aware of objects, relationships, and events by means of the senses, which includes such activities as recognising, observing, and discriminating* [4]. As 'perception' is closely connected to processes organising and interpreting the perceived information [4], we understand perceptions in the context of S&P as going beyond the mere sensory, also including some form of

subjective evaluation as described above. In contrast, 'emotions' are short-lived and relatively intense experiences [43]; they colour perceptions, influence decisions, and trigger behaviours [51]. Following that understanding, a few studies explored perceptions and emotions towards S&P from different disciplinary perspectives and for different target groups such as S&P professionals as compared to non-expert users.

Menges et al. [53] analysed public statements and survey data to explore employees' perceptions of and emotions towards IT staff, revealing patterns of negative language, perceived power imbalances, and mutual blame. Da Silva and Jensen [19] highlighted that perceptions of S&P professionals shape the role of the Chief Information Security Officer (CISO) as both a threat protector and a strategic advisor to management. Despite the significant influence of these perceptions on behaviour, detailed research on attitudes and emotions towards S&P professionals remains limited.

When it comes to S&P as a concept, Squires and Shade [69] examined S&P perceptions using ethnographic methods, finding that mismatched views between S&P professionals and employees, shaped by social relations and workplace practices, led to communication breakdowns and weakened the security link between people and technology. Da Silva and Jensen [19] found that S&P is often perceived as *mystical, unknown, and fearful* by CISOs and organisational leaders. Haney and Lutters [38] identified strategies from security advocates to address negative perceptions of S&P, such as building trust, enhancing communication, and incentivising positive behaviours.

A qualitative study inspired by political perception research [65] used sentence completion tasks (e.g., *My opinion on cybersecurity is that...*) to explore general perceptions of S&P. This study also found a generally negative stance towards cybersecurity, i.e., participants felt overwhelmed, scared, helpless, or confused, often attributed to its complexity. Yet, the authors argue that their results are not yet sufficient to inform behavioural interventions given the complexity and ambivalence of emotions.

To disentangle that complexity and to shed light on cybersecurity-related emotions, a recent literature review of 24 articles [78] explored the role of emotions and the often interchangeably-used terms 'affect' and 'mood' in the S&P context. First, the review shows that affect plays a central role in the field of cybersecurity. For example, van Schaik et al. [74] demonstrated an effect of affect heuristics on risk perception and Conrad et al. [18] found that notifications cause negative affect during internet browsing, regardless of their communication style. Second, the review revealed a trend towards negatively-valenced emotions. In particular, fear (e.g., [1, 16, 44, 83]), anxiety (e.g., [1, 7, 14, 16]) and sadness (e.g., [7, 10, 83]). Even so, only a few studies clearly differentiate between fear and anxiety (e.g., [1, 16, 63]).

A subsequent qualitative study with N=138 participants explored the complex interplay of antecedents and consequences of S&P-related emotions [77] based on the circumplex model of affect. The study highlighted various cybersecurity-relevant consequences across behavioural, cognitive and social dimensions, including negative tendencies such as avoidance behaviour, and unfavourable spill-over effects. Notably, positive high-arousal emotions, such as interest, have a positive impact on behavioural tendencies. Additionally, users expressed that security should be enjoyable to foster positive attitudes (including affective ones) and, ultimately, encourage positive behaviours [76]. Acknowledging this need, security and privacy education often incorporates elements of 'fun' (e.g., gamification) [8, 68]. Yet, there is still no clear understanding of which aspects truly promote 'fun' in the context of cybersecurity and privacy [76]. Prior results, however, highlight social dynamics as one of the major impacting factors on security attitudes and emotions [76, 77].

2.2 Social Dimensions of S&P

Das et al. [20] showed that social interactions significantly influence security behaviours, such as adopting secure authentication, updating passwords, and adjusting privacy settings. Their findings highlighted the effect of social triggers, with participants influenced by such interactions being four times more likely to share their behaviour and act as social triggers themselves. Further, Das et al. [23, 24] found that displaying the number of friends who adopted a Facebook security feature increased adoption likelihood. In another study, even non-personal social influence through crowd-sourced suggestions of Facebook users were influential in steering users' related S&P decisions [46]. Chen et al. [15] extended this work by designing phishing training that fostered social interaction through conversation-based and role-play-based methods. Both approaches improved anti-phishing self-efficacy and participants' intentions to seek support, reinforcing the value of social interactions in security education. As indicated by this work, social interactions in the form of conversations play a crucial role for shaping cybersecurity-related perceptions, emotions, and behaviours.

Initial research has thus explored how and why people engage in conversations about S&P. Das et al. [22] showed in an interview study that when S&P discussions arise, this is often to warn others, share protection strategies, or seek advice (e.g., when observing novel security tools or configuring new devices). They outline five social triggers that enhance security awareness, motivation, or knowledge: 1) observing others, 2) learning through discussions, 3) pranks and demonstrations, 4) experiencing security breaches, and 5) sharing device access. However, their findings suggest that security experts discussing related topics openly are sometimes perceived as paranoid, leading many to avoid such conversations to prevent being seen as socially inappropriate or preachy. In line with that, a related study by Gerber and Marky [35] found that security experts often hesitate to comment on or

intervene in others' security behaviour due to fear of negative reactions or uncertainty about their moral authority to judge such behaviour.

Rader et al. [61], replicated by Pfeffer et al. [58], demonstrated that stories serve as informal security lessons, influencing attitudes and behaviour. They found that security stories told in home settings are more likely to drive behaviour change than professional contexts, though stories shared by security-savvy individuals are more likely to be retold. In a subsequent analysis Rader and Wash [60] observed that experts and non-experts emphasise different aspects in security narratives: experts focus on attack mechanisms and prevention, while non-experts highlight who executed the attack and their motivations. Combining perspectives from both groups in conversations could address non-experts' knowledge gaps and foster more comprehensive understanding.

Furthermore, Das et al. [25] revealed that security news are typically shared out of responsibility, especially with friends and family, followed by significant others and colleagues. Gender differences emerged, with men being more likely to share security news out of responsibility, while those with lower security behavioural intentions shared news based on observing insecure behaviours. Lopez et al. [48] analysed conversations among security developers on platforms like Stack Overflow, revealing that exchanges increase awareness, enhance knowledge, and provide valuable assistance.

2.3 User Engagement

A variety of engagement strategies has been proposed in similar fields, where topics might be perceived as too complex or intimidating by lay users. For example, in mathematics, courses that target collaborative learning [54], enrichment classes that provide hands-on tasks and real-world applications of the topic [49], awareness campaigns that include, e.g., posters, public lectures, or articles in non-expert magazines [39], and gamified apps [45] have been found to increase engagement. Other examples include habit-building budgeting tools, that have been found to increase financial engagement and understanding [11, 33], and simulations that increase civic engagement [6, 67]. Further, storytelling has been found to help making complex topics more approachable and increase engagement in domains such as health policy [80] and environmental science [3]. S&P share similar barriers of perceived complexity and disengagement as those topics, while also carrying great emotional weight and personal risk, often evoking fear or avoidance, which makes engagement particularly challenging.

2.4 Implications for this Research

Previous research has demonstrated connections between S&P-related social interactions, perceptions, emotions, and behaviours across various disciplines. For instance, perceptions of S&P influence the roles of professionals, such as CISOs, and how they are viewed within organisations [19]. Negative emotions can impact both thinking and motivation to adopt secure practices [58]. Moreover, much of the existing work paints a negative view of S&P, portraying it as complex, fearful, and even mystical [19, 38, 63], with emotions like fear, anxiety, and sadness commonly reported in response to S&P issues [7, 16, 83].

We build on this work and shift the focus towards positive S&P associations, striving to identify pathways to counter negative emotional responses and ultimately increase user engagement and experience in the S&P context. For this, we asked our participants what would make S&P more fun. Fun is a recognised hedonic quality in User Experience (UX) [27] that can help to make complex topics like S&P more approachable. We particularly selected fun as a high-arousal form of enjoyment, as such emotions have been found to foster secure behaviour [77]. By asking what would make S&P *more* fun, we also seek to identify barriers for enjoyment.

Further, while social interactions in the form of conversations, including stories and anecdotes, have been found successful in triggering secure behaviour, research so far has been limited on identifying conversation barriers for S&P expert users. Our study extends prior findings in identifying obstacles and potential facilitators for S&P conversations also among non-expert users. This exploration will lay the groundwork for future research, enabling the development of more holistic human-centred S&P interventions that consider socio-emotional influences and responses.

3 Method

We used an online survey hosted on SoSciSurvey with a representative sample of $N = 496$ U.S. citizens to explore how to make S&P more enjoyable and what facilitates conversations on that context. The sample was recruited via Prolific. All participants were reimbursed with an hourly rate of $13, based on a 20-minute duration (average time $M = 19.5$ minutes, $SD = 8.21$, $Med = 18$). We included two simple attention checks. The study was pre-tested with 10 participants who were also recruited via Prolific. The pre-test comments only concerned typos and sentence structure, which we used to refine the survey.

3.1 Ethical Considerations

All recommendations for conducting studies with human participants provided by our university's ethics commission were met. We followed their provided checklist and the APA guidelines for ethical psychological research involving humans [5]. As such, all participants were informed about the study purpose and procedure prior to giving their consent. They had the right to withdraw from the study at any time and also to have their data deleted after they had completed the study.

We did not collect personally-identifiable information. All demographic questions were voluntary and age was collected in ranges instead of exact age to further enhance anonymity. All data was stored on German servers that are subject to strict EU data protection law. Participation was voluntarily and participants were reimbursed with an hourly rate of $13, which exceeded minimum wage in the U.S. at the time the study was conducted and in line with the Prolific platform's recommendations for fair payment[1].

3.2 Procedure

The study comprised six main steps, as visualised in Figure 1. More details and all questions are provided in Appendix A:

First, the participants were asked for informed consent.

Second, we used open text questions to capture general privacy perceptions. For this, we asked our participants:

- to complete the sentences *Privacy is a topic that...* and *It would be so much more fun to protect my (digital) privacy if....*
- to imagine that (digital) privacy was a person (more specifically, a colleague of theirs) and to provide three character traits they would use to describe this person.
- to indicate how well they protected their privacy, as compared to other people in their social circle, such as their colleagues, friends, or parents, using a slider on a scale ranging from *less* to *more*.

While the first points target at measuring the participants' beliefs, the last point assesses self-reported behaviour [31].

Third, we repeated the questions from the second block for IT security.

Fourth, we focused on S&P conversations, asking them to indicate how often they talked to other people about: (1) privacy issues, and (2) IT security issues on a scale ranging from "1=very infrequently" to "7=very frequently" with *never* as a fallback option. We then asked the participants to rate different reasons for not talking to others frequently about privacy on a 7-Point Likert scale (with 1=strongly disagree and 7=strongly agree) based on answers given in an interview study on that topic by Gerber and Marky [35]. Then, the participants were asked to finish the sentence *I would talk about privacy much more often with others if....* The last two questions were repeated for IT security.

Fifth, we asked about perceptions of S&P-savvy people. We used a 7-Point Likert scale to indicate whether our participants thought that people who used different strategies to protect their S&P, including, e.g., encrypting their devices or refraining from using social media, were paranoid. Again, the answers were selected based on Geber and Marky [35]. This was followed by the Nerd-Genius scale [70] on people protecting their privacy (in the first question) and their IT security (in the second question). This scale asks about stereotypes typically associated with *nerds* or *geniuses*, such as being socially awkward, obsessed with computers, or gifted in math.

Sixth, we asked for several S&P-related and general demographics, using two questions based on Nthala and Flechais [55] to assess S&P skills and security support for other people, the ATI scale [32] to capture technical affinity, the Security Attitude scale (SA-6) [30] to measure security attitudes, the Internet Users' Information Privacy Concerns scale (IUIPC-8) [36, 50] to measure privacy concerns, and the technical sub scale of the Online Privacy Literacy Scale (OPLIS) [73] to assess privacy literacy. Finally, we asked for gender, age, education, and employment status, thanked our participants, and redirected them to Prolific.

3.3 Sample

We recruited a sample representative of the adult U.S. population via Prolific. A total of 511 participants completed the questionnaire, of whom 15 were excluded since they failed at least one of the two attention checks. Our final sample thus included 496 participants. Of those, 258 were women, 234 men, 2 agender, and 1 non-binary. For the participants' detailed demographics and skills and attitudes with regard to S&P, the reader is referred to Tables 1 and 2.

3.4 Limitations

We conducted a survey study that provided a large, diverse sample, but the qualitative data may not be as rich as that from in-depth interviews. Future studies can enrich our understanding of how S&P are perceived as a concept by pursuing alternative study designs such as interviews or experience sampling. In addition, we relied on self-reported data, which might be affected by social desirability or false recalls. We further focused on the U.S. population, for which Prolific provides the opportunity to recruit a sample that is representative in terms of age, sex, and ethnicity. The S&P perception might be different for people with other cultural backgrounds, since, for example, people in the U.S. may value different aspects in terms of privacy than people in Europe [79]. Furthermore, although balanced in terms of age, sex, and ethnicity, our sample may not be representative with regards to other sociodemographic characteristics, such as being slightly skewed towards users with a Bachelor's degree [13]. This might have influenced our findings, as, for example, individuals with higher education levels have been found to rely less on automated tools for security guidance [62].

[1] https://www.prolific.com/calculator

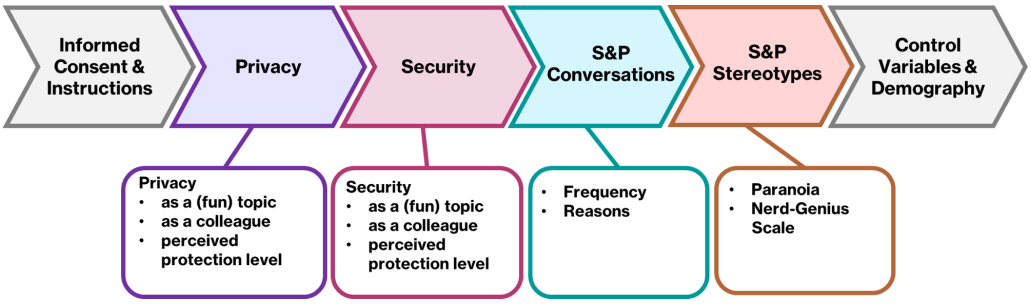


Figure 1: Visualisation of the study procedure.

Age in years: N (%)	Education: N (%)	Employment: N (%)
18-20: 30 (6.1%)	School student: 6 (1.2%)	Employed full time: 182 (36.7%)
21-25: 44 (8.9%)	High School Diploma: 156 (31.5%)	Employed part-time: 64 (12.9%)
26-30: 50 (10.1%)	Bachelor's Degree: 186 (37.5%)	Unemployed and on the lookout: 41 (8.3%)
31-35: 44 (8.9%)	Master's Degree: 78 (15.7%)	Unemployed and not on the lookout: 13 (2.6%)
36-40: 39 (7.9%)	Ph.D. or higher: 21 (4.2%)	Student: 41 (8.3%)
41-45: 42 (8.5%)	Other: 48 (9.7%)	Retired: 66 (13.3%)
46-50: 43 (8.7%)		Homemaker: 20 (4%)
51-55: 42 (8.5%)		Self-employed: 50 (10.1%)
56-60: 64 (12.9%)		Incapacitated for work: 10 (2%)
61-65: 52 (10.5%)		Other: 4 (0.8%)
66-70: 25 (5.0%)		
>70: 2 (4.2%)		

Table 1: Participants' demographic values.

3.5 Data Analysis

The open-text responses were analysed using thematic analysis [12]. Two authors initially coded 20% of the responses independently and iteratively developed a codebook. They then discussed and agreed on a unified codebook. Given the simplicity of many responses, such as short text snippets or one-word answers, we followed Ortloff et al.'s recommendations [56]. One author coded all responses using the agreed codebook and added new codes as necessary. The second author reviewed the codings, and noted discrepancies, and the authors then resolved these through discussion, refining the codebook and adding new codes. The first author subsequently re-coded the responses using the updated codebook. The codebook is available in Appendix B.

4 Results

This section presents findings on the perceptions of S&P in terms of associations, protection measures, conversations, and stereotypes. We report the frequency of notions for each code with *s* for security-related and *p* for privacy-related notions.

4.1 S&P-related Associations

S&P was most often described as **important** (s=144 (29.03%), p=226, (45.56%)), yet only few participants also found it interesting (s=22 (4.44%), p=11 (2.22%)), e.g.:

> *"Security is really uncool but really important."* (P305)

Instead, participants highlighted the **complexity** and overwhelming nature of S&P (s=57 (11.49%), p=16 (3.23%)), and reported feelings of **worry and fear** (s=17 (3.43%), p=36 (7.26%)) in line with previous results [19, 47, 65, 77], e.g.:

> *"[Security is a topic that] invokes fear and concern."* (P417); *"[Security is a topic that] sounds scary."* (P159)

For security, these feelings were associated with severe **knowledge and experience gaps** (s=83 (16.73%)) mirroring prior research [47, 65, 77]. Interestingly, hardly any participants reported to have limited privacy knowledge (p=4 (0.81%)). Instead, privacy was described as a **controversial** and thus sensitive topic (p=31 (6.25%)). Although S&P was generally not perceived as particularly engaging, only a small number of participants explicitly characterised it as **uninteresting or boring** (s=17 (3.43%), p=11 (2.22%)), contrary to

S&P skill: N (%)	ATI scale	SA-6	IUIPC-8			OPLIS
			Control	Awareness	Collection	
Novice: 158 (31.9%)	M=3.37	M=3.15	M=5.86	M=6.30	M=5.86	M=3.85
Competent: 308 (62.1%)	SD=1.01	SD=0.95	SD=1.22	SD=1.02	SD=1.20	SD=1.27
Expert: 30 (6%)	Med=3.33	Med=3.17	Med=6.00	Med=7.00	Med=6.25	Med=4.00
	Min=1.11	Min=1.00	Min=1.00	Min=1.00	Min=1.00	Min=0.00
	Max=6.00	Max=7.00	Max=7.00	Max=7.00	Max=7.00	Max=5.00

Table 2: Participants' level of S&P skills and attitudes.

prior assumptions [38], and thus something they do not wish to discuss, e.g.:

> *"Security is a topic I am sick of hearing about."* (P192)

Our data showed disagreement about the attention paid to S&P: While privacy was noted as a current **public interest** topic by several participants (p=37), a larger number of participants demanded **greater attention** to S&P (s=63 (12.70%), p=91 (18.35%)) – an obstacle also identified previously [35, 38], stating it should be more frequently discussed (s=22 (4.44%), p=27 (5.44%)) or taken more seriously (s=41 (8.27%), p=64 (12.90%)), e.g.:

> *"[Security] gets a lot of publicity, but not enough attention"* (P236); *"If we are not willing to talk openly about [privacy] we will continue to lose it."* (P179)

4.2 How to Make S&P Fun

Participants provided several insights on making S&P protection more engaging.

Simplification was key to enjoyment, with participants frequently emphasising the need to reduce complexity (s=116 (23.39%), p=103 (20.77%)). In that same vein, many participants blamed **inadequate knowledge** for S&P not being fun (s=89 (17.94%), p=35 (7.06%)), e.g.:

> *"It would be more fun to protect my IT security if I learned more about it."* (P5)

This complexity also contributed to perceptions that S&P was not **accessible** enough to be enjoyable (s=73 (14.72%), p=84 (16.94%)), with participants criticising cumbersome processes and costs (s=20 (4.03%), p=11 (2.22%)).

Participants also expressed a strong desire for enhanced **self-efficacy**, seeking greater control over their data security and visibility online (s=33 (6.65%); p=46 (9.27%)), and highlighting the importance of feeling that their actions could make a meaningful impact (s=26 (5.24%), p=51 (10.28%)), e.g.:

> *"If there was tangible proof that my efforts kept my data secure."* (P467)

Conversely, a substantial proportion of participants viewed the complete **relinquishment of responsibility** for their S&P as the only viable solution (s=75 (15.12%), p=111 (22.38%)). They favoured either reliance on automated systems (s=9, p=16) or the transfer of responsibility to competent peers or institutions such as the government (s=20 (4.03%), p=29 (5.85%)), e.g.:

> *"If government and internet providers did more to secure the internet."* (P473)

Some participants emphasised the emotional dimension, identifying **negative emotions** as a barrier to making S&P enjoyable (s=21 (4.23%), p=24 (4.84%)), e.g.:

> *"If it was not talked about in such a doomsday way."* (P185)

Surprisingly, relatively few participants proposed **gamification** or similar engaging methods as a way to enhance the enjoyment of S&P (s=16 (3.23%), p=27 (5.44%)). Still, several participants advocated for **incentives**, including monetary rewards (s=27 (5.44%), p=30 (6.05%)), e.g.:

> *"If we got cake every month there were no breaches."* (P317)

Although only a minority, some participants perceived S&P as **too serious** to be made enjoyable (s=8 (1.61%), p=16 (3.23%)), while others felt that **nothing** could make S&P fun (s=20 (4.03%), p=11 (2.22%)).

Figure 2: Character traits associated with privacy.

Figure 3: Character traits associated with security.

4.3 S&P Character Traits

Participants were asked to describe privacy and security as if they were people, assigning three character traits to each (see Figure 2). Both privacy and security were predominantly associated with **positive** traits such as *trustworthy* (s=60 (12.10%), p=111 (22.38%)), *reliable* (s=105 (21.17%), p=82 (16.53%)), *honest* (s=32 (6.45%), p=67 (13.51%)), *good* (s=21 (4.23%), p=26 (5.24%)), and *helpful* (s=29 (5.85%), p=17 (3.43%)), indicating a promising receptiveness towards the topic. Security, however, was more often characterised as **intelligent**, with traits like *smart* (s=88 (17.74%), p=26 (5.24%)) and *knowledgeable* (s=26 (5.24%), p=0 (0%)), confirming that security is perceived as a topic that warrants expertise and knowledge. Both were also perceived as *strong* (s=47 (9.48%), p=40 (8.06%)) and *secure* (s=61 (12.30%), p=44 (8.87%)).

Neutral traits were also common. Privacy was described as *introverted* (n=88 (17.74%)), *discrete* (n=33 (6.65%)), and *secretive* (n=28 (5.65%)), while security was labelled *quiet* (n=37 (7.46%)) and *changing* (n=32 (6.45%)). A smaller subset of traits had **negative** connotations, with privacy described as *complicated* (n=47 (9.48%)), *hypocritical* (n=36 (7.26%)), and *unreliable* (n=19 (3.83%)), stressing the need to reframe privacy debates. For security, the most frequent negative trait was also *complicated* (n=63 (12.70%)), followed by *boring* (n=24 (4.84%)) and *suspicious* (n=18 (3.63%)), underscoring the need to reframe security in a more positive and approachable manner. Full coding is available in Appendix B.

4.4 Perceived Level of S&P Protection

The majority of participants rated themselves as **above average** in protecting both security and privacy (see Figures 4 and 5), perhaps reflecting overly optimistic self-perceptions. Most considered their protection skills slightly better than their partner's but significantly better than those of children, siblings, friends, and acquaintances. Notably, participants felt they protected their privacy much better than colleagues, though they saw only a slight advantage in IT security. This may reflect shared workplace security protocols. Parents were consistently rated as the least capable in both categories.

To explore how participants' skill levels and target types influence the perceived level of security and privacy protection, we fitted two linear mixed-effects models. The analyses revealed a main effect of skill level for privacy ($F(2,2808.94) = 39.16$, $p < .001$, $\eta_p^2 = .03$) and security protection ($F(2,2752.47) = 94.30$, $p < .001$, $\eta_p^2 = .06$), indicating that self-assessed expertise is positively related to perceived protection. We further found a main effect of target type for privacy ($F(6,898.94) = 3.99$, $p < .001$, $\eta_p^2 = .03$) and security protection ($F(6,770.10) = 4.06$, $p < .001$, $\eta_p^2 = .03$). The analyses did not yield significant interaction effects ($F(12,882.63) = 0.62$, $p = .827$ for privacy; $F(12,765.73) = 0.25$, $p = .995$ for security), indicating that skill level affects all target types similarly.

Post-hoc comparisons using paired samples t-tests with Bonferroni-Holm corrections indicate that participants self-reported significantly stronger privacy protection when comparing themselves to all other targets than when comparing themselves to their partner, possibly reflecting perceived shared values between partners. Further, participants reported significantly stronger privacy protection when comparing themselves to acquaintances than to colleagues, siblings, children, and friends, and when comparing themselves to their parents than to their siblings and children. It is possible that participants perceive people who are closer to them as more similar, which may also influence the evaluation of their level of protection. To test whether self-assessed skills align with privacy literacy, we calculated a Kruskal-Wallis test, which confirmed an effect of skill level on privacy literacy measured via OPLIS ($\chi^2(2) = 51.10$, $p < .001$, $\eta^2 = .10$). Post-hoc Wilcoxon ranked-sum tests with Bonferroni-Holm corrections confirmed that participants with higher self-assessed expertise had higher levels of privacy literacy.

Further, participants reported significantly stronger security protection when comparing to their parents than to all other targets, possibly indicating perceived knowledge gaps among older users. Comparable to privacy protection, participants reported significantly stronger security protection when comparing themselves to acquaintances than to colleagues, siblings, their partner, and friends, and when comparing themselves to friends than to colleagues and their partner. To examine whether self-assessed skill levels align with security attitudes, we conducted a Welch's ANOVA, revealing a significant effect of skill level on security attitude as measured by the SA-6 scale, $F(2,493) = 68.21$, $p < .001$, $\eta_p^2 = .22$. Follow-up independent-samples t-tests with Bonferroni-Holm corrections showed that participants with higher self-assessed expertise reported significantly stronger security attitudes.

The detailed results for the post-hoc comparison analyses are provided in Appendix B.

4.5 S&P Conversations

Around half of participants reported discussing privacy issues **infrequently**, with even fewer discussing security (see Fig-

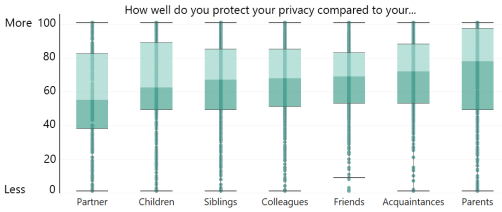


Figure 4: Boxplots showing the data distribution regarding how well participants think they protect their privacy compared to their peers and family.

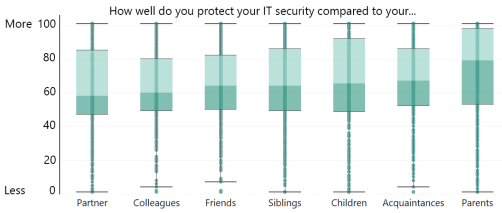


Figure 5: Boxplots showing the data distribution regarding how well participants think they protect their IT security compared to their peers and family.

ure 6). Common reasons were the lack of relevant conversation starters, perceived complexity, or disinterest from others (see Figures 8 and 7) extending prior literature identifying lack of interest, social aspects, lack of resources/opportunities and lack of legitimacy [35]. However, contrasting results by Gerber and Marky [35], most participants disagreed with the idea that they themselves lacked interest or that they feared negative reactions when raising these topics. Two ANOVAs showed a main effect of self-reported skill level on conversation frequency for privacy ($F(2,460) = 13.74$, $p < .001$, $\eta_p^2 = .06$) and security ($F(2,432) = 36.29$, $p < .001$, $\eta_p^2 = .14$). Post-hoc tests using independent sample t-tests with Bonferroni-Holm corrections revealed that self-identified experts talk more frequently about S&P than participants who consider themselves to be novices or competent, while participants who consider themselves to be competent talk more frequently about S&P than self-identified novices. The detailed results for the post-hoc comparison analyses are provided in Appendix B.

Our qualitative analysis, based on responses to the prompt *I would talk about security/privacy much more often if...*, confirmed the quantitative findings regarding conversation barriers. Such barriers for S&P conversations included **knowledge gaps**. While many participants felt they themselves lacked sufficient knowledge (s=140 (28.23%), p=64 (12.90%)), others felt peers lacked understanding (s=33 (6.65%), p=26 (5.24%)):

Figure 6: Answers to statements about the frequency with which participants talk to others about privacy and IT security issues.

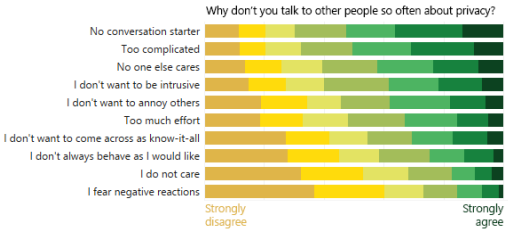


Figure 7: Answers to statements about reasons for not talking frequently with others about privacy, based on Gerber and Marky [35].

> *"If they could relate. Sometimes they don't understand what I'm talking about."* (P123)

Interestingly, considerably more participants thought others were **not interested** (s=63 (12.71%); p=65 (13.10%)) in the topic than reporting disinterest themselves (s=17 (3.43%), p=13 (2.62%)), e.g.:

> *"If others were as interested in the subject as me."* (P39)

Participants also noted **social norms** (s=50 (10.08%), p=80 (16.13%)), where security and privacy were seen as uncommon topics to address (s=30 (6.05%); p=47 (9.48%)), or only worth discussing with those sharing similar knowledge or interest (s=20 (4.03%); p=47 (9.48%)). For privacy especially, some participants felt it was socially unacceptable to bring it up (p=27 (5.44%)), e.g.:

> *"I would talk about privacy more often if it wasn't taboo."* (P66)

Additionally, the **perception** of S&P as negative and complex (s=33 (6.65%); p=30 (6.05%)), or uncontrollable and thus futile to discuss (s=14 (2.82%); p=18 (3.63%)) further hindered conversations, e.g.:

> *"Just talking about it without being able to do anything is just stressful."* (P284)

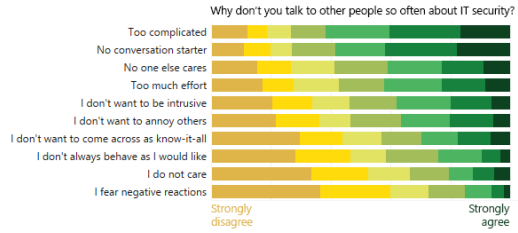


Figure 8: Answers to statements about reasons for not talking frequently with others about IT security, based on Gerber and Marky [35].

Finally, participants highlighted a **need for conversation facilitators** (s=104 (20.97%); p=127 (25-60%)), such as others initiating discussions (s=43 (8.67%), p=67 (13.51%)) or external triggers like media coverage or workplace training (s=61 (12.30%), p=60 (12.10%)).

4.6 S&P Stereotypes

Most participants did **not** perceive individuals who follow basic security practices – such as using antivirus software or regularly updating devices – as **paranoid** (see Figure 9). However, behaviours such as covering device cameras, avoiding social media, reading privacy policies, and encrypting devices were more likely to be viewed as paranoid, reflecting differing connotations associated with security and privacy protection behaviours.

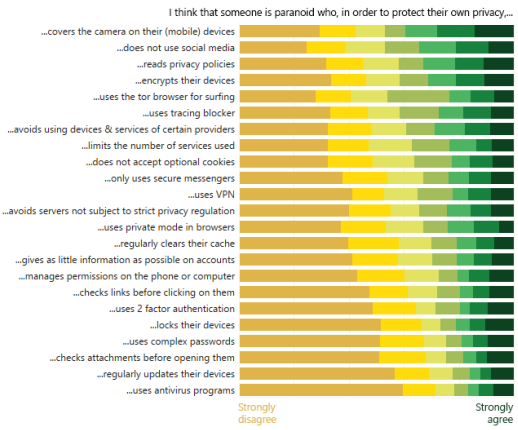


Figure 9: Answers to statements about whether someone is paranoid who uses privacy protection measures, based on Gerber and Marky [35].

Utilising the Nerd-Genius scale [70], we assessed the stereotypes attributed to individuals who actively protect their privacy and security. This scale includes traits associated with both *geniuses* and *nerds*. Participants predominantly associated these individuals with *genius* traits, such as intelligence, genius-level aptitude, computer obsession, and mathematical proficiency (see Figure 10 and 11), again underscoring the perception of S&P as a complex topic that warrants high levels of expertise. The trait 'introvert' from the *nerd* category received the highest agreement, though fewer than 25% strongly or somewhat agreed with this attribution. The results provide a promising foundation for bridging the gap between experts and lay users and fostering a more positive interaction between them.

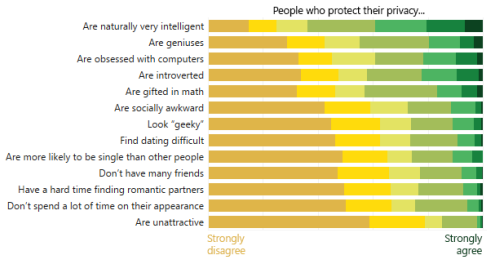


Figure 10: Answers to the Nerd-Genius scale [70] capturing perceptions of people who protect their privacy.

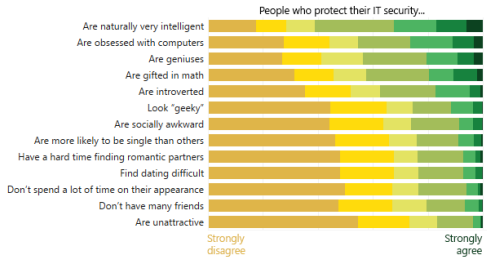


Figure 11: Answers to the Nerd-Genius scale [70] capturing perceptions of people who protect their IT security.

5 Discussion

In the following sections, we discuss our overall findings and additional relevant findings and also practical implications with regard to the RQs.

S&P is perceived as negative yet important. Consistent with previous studies, our research reveals mixed perceptions of S&P. Participants acknowledged its importance but also found it complex, overwhelming, and frightening, aligning with findings from Renaud et al. [65] and Da Silva and Jensen [19]. This complexity and associated fear underscore the need to address the emotional and social dimensions of S&P research. While fear has been a focus in prior studies [1, 16, 44, 83], efforts to reduce fear and foster positive emotions are still scarce [78]. Our findings on suggested measures for fostering positive user engagement with S&P align with Haney and Lutters' [38] strategies, highlighting trust-building, engaging conversations, and incentivisation. In summary, our findings suggest that S&P needs to be more engaging and enjoyable to address current negative perceptions. While gamification intuitively appears to be a promising solution, perceptions of gamifying S&P were mixed.

Gamification of S&P topics is ambiguous. Surprisingly, while gamification is often associated with enhancing user engagement, it was mentioned infrequently by participants. Instead, they emphasised the need for reducing complexity and improving usability. This suggests a greater focus on making S&P solutions more user-friendly rather than simply adding gamified elements. A minority of participants even expressed the view that S&P should not, or cannot, be made fun, indicating that it should not be gamified. This sentiment may reflect concerns about diminishing the seriousness of the topic or deep-seated negative perceptions, suggesting a need for further investigation into these attitudes.

Overall, the results indicate that addressing pragmatic usability aspects – such as efficacy and ease of use – may be more crucial than introducing fun or hedonic elements. Gamification alone may not enhance engagement if underlying usability issues are not resolved. This reflects the distinction between pragmatic usability, which concerns task efficiency, and hedonic usability, which relates to aspects like fun and stimulation [40]. Addressing users' hedonic needs may be ineffective or even counterproductive if basic usability requirements are not met. When users feel stressed or out of control, introducing stimulating elements that elevate arousal could exacerbate negative experiences rather than enhance engagement. Participants' preference for usability improvements over gamification suggests that not all users or S&P contexts may benefit from gamification. Perhaps S&P is not automatically fun when a gamified element is introduced, while it might well be fun in training scenarios. Future research should explore the balance between gamification and usability enhancements, particularly in different S&P scenarios.

Additionally, the desire for more control over personal data versus automation or externalisation of S&P tasks indicates a mixed preference for responsibility management, aligning with Renaud et al.'s [64] findings on de-responsibilisation.

Security and Privacy are not articulated – but for different reasons. While participants personally expressed interest in discussing S&P, they assumed that others were disinterested, resulting in a collective silence on the topic.

Privacy discussions were further constrained by social norms and the topic's controversial nature, drawing parallels to politics or religion. Participants feared negative reactions or being perceived as overly cautious, leading them to avoid conversations on privacy even when recognizing its importance. In contrast, security was rarely discussed due to a lack of knowledge rather than controversy. This distinction suggests different barriers to engagement: while privacy discussions are hindered by social discomfort and fear of judgment, security discussions are avoided due to knowledge gaps.

Yet, even though the participants rated their own knowledge and experience levels as low, they consistently perceived their level of protection to be greater than other family members, friends or colleagues. This hints at a potential mismatch between their perceived and their actual level of protection compared to others or the illusory superiority effect [75] manifesting in yet another domain. Participants indicated that S&P would be more engaging if they had more knowledge. This suggests a need for improved S&P education integrated into curricula and for engaging interactive experiences as proposed by Wiederhold [81]. Based on our findings, S&P education measures in school curricula and workplace trainings should use positive formats like role-play to reduce intimidation and build confidence.

Security advocates are intelligent whereas privacy advocates are paranoid? By differentiating between security and privacy, our study uncovered distinct perceptions for each construct, highlighting the need to address these differences in both research and organisational measures. Participants perceived security-related measures (e.g., antivirus software, device updates) as less paranoid than privacy-focused actions (e.g., covering cameras, avoiding social media). Notably, security was more frequently associated with intelligence and expertise, while privacy was linked to traits like introversion, discreteness, or secretiveness, reflecting the more personal and intimate nature of privacy concerns.

These findings have implications for organisational S&P initiatives, such as appointing "security champions" or "privacy champions" [34, 37, 72]. While research already established that the approach comes with its own challenges, e.g., related to the selection of appropriate people [9, 34] and lack of management support [37], our research indicates that security as compared to privacy champions might need to be introduced and supported differently. Specifically, privacy champions may need assistance in countering stereotypes that frame privacy-conscious behaviours as overly cautious or secretive and in reinforcing the legitimacy and importance of privacy measures within the organisation. This could involve targeted training, executive endorsement, and strategic

communication to shift organisational perceptions and ensure privacy initiatives receive the same level of recognition and support as security measures. The same likely applies to data protection officers, i.e., the people responsible to advocate for, check compliance with, and consult on privacy-related topics. They might benefit from strategic communication explaining the value of privacy measures beyond mere compliance, e.g., highlighting privacy as a business case for new products or the potential reputation loss and costs associated with data leaks in case of insufficient privacy considerations.

5.1 Conclusion & Recommendations

Our findings reveal a surprising and simple way to enhance engagement with S&P through initiating S&P-related conversations. Six key points emerge:

Fostering positive engagement with S&P. Consistent with previous research, our study reveals mixed feelings towards S&P. Positive perceptions generally highlight the importance of S&P and associate it with professionalism and intelligence. Conversely, negative perceptions focus on complexity, mysticism, ambiguity, and frustration. This dichotomy suggests that while S&P may be valued on a general level, personal experiences with S&P are often negative. Future work should explore this distinction further, focusing on enabling users to make positive social and emotional experiences with S&P. The framework developed by Faklaris et al. [29] can provide initial guidance on what type of social influence to use in which step of S&P learning and adoption. For example, storytelling might be helpful for raising threat awareness whereas social proof may better support S&P learning. Further, strengthening users' self-efficacy by highlighting the security relevance of everyday actions like device locking or updating and promoting security practices like password managers and 2FA as empowering choices rather than obligatory tasks may help to overcome fears and negative perceptions.

Integrating S&P conversations into work routines. Although individuals express a willingness to discuss S&P with peers, they often perceive others as uninterested and lack conversation starters. This gap, also identified by Gerber and Marky for expert users [35], suggests that fostering S&P discussions could be beneficial. Examples of positive effects on S&P behaviours triggered by peer influence through conversations are also summarized by Wu et al. [82]. The workplace presents an opportunity to foster more organic S&P discussions. Initiatives such as workplace S&P meet-ups, public awareness days (e.g., Safer Internet Day), or integrating S&P elements into unexpected settings (e.g., on frequently used office material or informational posters) might stimulate S&P conversations. For example, routine security updates could be utilised as conversation starters, e.g., by encouraging a collective coffee break when updates are installed. In this break, employees could casually discuss the necessity and benefits of updates and other security measures. Such low-stakes, structured interactions could normalise S&P discussions and reduce perceived barriers.

Integrating S&P conversations beyond on-site work places. As work does not only happen in classical on-site settings any more and is increasingly intertwined with private life, it is also important to consider remote and private settings. Widely used services such as Google services and apps such as messenger apps or social media platforms offer options for peer-to-peer learning and informal exchange in everyday interactions. For example, private persons as well as remote workers participating in team communications online could be reached through integrated prompts in meetings or chat platforms. In-person discussions in private contexts among friends or family could be triggered through many ways including cybersecurity education in schools, poster campaigns in public settings such as bus stops, or through prompts integrated in everyday objects such as water bottle labels.

Making privacy protective practices less paranoid. Privacy, in particular, may benefit from a cultural shift within organisations to counteract the view of privacy as "paranoid". A strong error culture, psychological safety, and visible support from leadership could help reduce shame, and guilt associated with privacy-related mistakes. Likewise, increasing privacy visibility might help in reducing social taboos around the topic, e.g., through media coverage also in entertainment formats, highlighting privacy features in apps and devices, and legal framings that treat privacy as a valuable and achievable goal rather than an abstract ideal.

Supporting calibration of perceived vs. actual protection levels. Participants tended to overestimate their S&P knowledge compared to others, reflecting the illusory superiority effect [75] or optimism bias [66]. Similar to overestimations in driving ability [26], individuals rated their S&P protection as superior to that of their peers. To address this, providing realistic assessments of one's protection level and incorporating social cues (e.g., social password meters or visibility of friends' security practices) could help align perceptions and motivate improvements in S&P.

Fostering interactions between experts and lay users. Positive perceptions of S&P-conscious individuals, who were associated with genius but not nerd attributes in our study, point towards untapped potential of facilitating interactions between S&P experts and lay users to leverage expert knowledge more effectively, potentially improving S&P practices privately and within organisations. Positioning S&P professionals as approachable role models could encourage broader engagement and reduce the perceived exclusivity of S&P discussions, which are often confined to expert circles.

Acknowledgments

This research work has partially been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

Data Availability Statement

Due to the high sensitivity of survey data with regards to the potential identification of participants, we do not make the data publicly available. Detailed information on the sample, the survey guide, codebook, and exemplary quotes are provided in the Appendix. For further information or access to the original survey data, please contact the authors.

References

[1] H. Abroshan, J. Devos, G. Poels, and E Laermans. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, 9:121916–121929, 2021. https://doi.org/10.1109/ACCESS.2021.3109091.

[2] Krishnashree Achuthan, Sugandh Khobragade, and Robin Kowalski. Public sentiment and engagement on cybersecurity: Insights from reddit discussions. *Computers in Human Behavior Reports*, 17:100573, 2025.

[3] Karolin Andersson, Anneli Sundin, and Robert Watt. Rethinking communication: integrating storytelling for increased stakeholder engagement in environmental evidence synthesis. *Environmental Evidence*, 7(6), 02 2018.

[4] APA. APA Dictionary of Psychology, 2023. Retrieved 16 February 2023 from: https://dictionary.apa.org/perception.

[5] American Psychological Association. Ethical principles of psychologists and code of conduct. 2016.

[6] Christine Bachen, Pedro Hernández-Ramos, Chad Raphael, and Amanda Waldron. Civic play and civic gaps: Can life simulation games advance educational equity? *Journal of Information Technology & Politics*, 12, 11 2015.

[7] Eric Bachura, Rohit Valecha, Rui Chen, and H Raghav Rao. The OPM Data Breach: An Invesitigation of Shared Emotional Reactions on Twitter. *MIS Quarterly*, 46(2):881–910, 2022. https://doi.org/10.25300/MISQ/2022/15596.

[8] Ryan J Baxter, D Kip Holderness Jr, and David A Wood. Applying basic gamification techniques to it compliance training: Evidence from the lab and field. *Journal of information systems*, 30(3):119–133, 2016.

[9] Ingolf Becker, Simon Parkin, and M. Angela Sasse. Finding security champions in blends of organisational culture. In *Proceedings of the 2nd European Workshop on Usable Security*. Internet Society, 2017.

[10] O. Beris, A. Beautement, and M. A. Sasse. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In A. Somayaji, R. Böhme, P. van Oorschot, and M. Mannan, editors, *Proceedings of the 2015 New Security Paradigms Workshop*, page 73–84, 2015. https://doi.org/10.1145/2841113.2841119.

[11] Paula Bitrián Arcas, Isabel Buil, and Sara Catalán. Making finance fun: the gamification of personal financial management apps. *International Journal of Bank Marketing*, 39:1310–1332, 06 2021.

[12] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. https://doi.org/10.1191/1478088706qp063oa.

[13] United States Census Bureau. Census Bureau Releases New Educational Attainment Data, 2023. Retrieved 19th May 2025 from: https://www.census.gov/newsroom/press-releases/2023/educational-attainment-data.html.

[14] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4):1228–1247, 2019. https://doi.org/10.1287/isre.2019.0860.

[15] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[16] Violet Cheung-Blunden, Kiefer Cropper, Aleesa Panis, and Kamilah Davis. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion*, 19(8):1353–1365, 2019. https://doi.org/10.1037/emo0000508.

[17] Kevin Collier. Ransomware attack delays patient care at hospitals across the U.S., 2022. Retrieved 15th November 2022 from: https://www.nbcnews.com/tech/security/ransomware-attack-delays-patient-care-hospitals-us-rcna50919.

[18] Colin Conrad, Jasmine Aziz, Natalie Smith, and Aaron Newman. What Do Users Feel? Towards Affective EEG Correlates of Cybersecurity Notifications. In *NeuroIS Retreat*, pages 153–162. Springer, 2020. https://doi.org/10.1007/978-3-030-60073-0_17.

[19] Joseph Da Silva and Rikke Bjerg Jensen. "cyber security is a dark art": The ciso as soothsayer. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), November 2022.

[20] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. A typology of perceived triggers for End-User security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 97–115, Santa Clara, CA, August 2019. USENIX Association.

[21] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. The security & privacy acceptance framework (spaf). *Foundations and Trends® in Privacy and Security*, 5(1-2):1–143, 2022.

[22] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, Menlo Park, CA, July 2014. USENIX Association.

[23] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 739—-749, New York, NY, USA, 2014. Association for Computing Machinery. https://doi.org/10.1145/2660267.2660271.

[24] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. The role of social influence in security feature adoption. In *Proceedings of the Conference on Computer Supported Cooperative Work & Social Computing*, CSCW '15, pages 1416—-1426, New York, NY, USA, 2015. Association for Computing Machinery. https://doi.org/10.1145/2675133.2675225.

[25] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1—12, New York, NY, USA, 2018. Association for Computing Machinery.

[26] David M DeJoy. The optimism bias and traffic accident risk perception. *Accident Analysis & Prevention*, 21(4):333–340, 1989. https://doi.org/10.1016/0001-4575(89)90024-9.

[27] Sarah Diefenbach, Nina Kolb, and Marc Hassenzahl. The 'hedonic' in human-computer interaction: history, contributions, and future research directions. In *Proceedings of the 2014 Conference on Designing Interactive Systems*, DIS '14, page 305–314, New York, NY, USA, 2014. Association for Computing Machinery.

[28] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), 11 2018.

[29] Cori Faklaris, Laura Dabbish, and Jason I. Hong. A framework for reasoning about social influences on security and privacy adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery.

[30] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. A Self-Report measure of End-User security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 61–77, Santa Clara, CA, August 2019. USENIX Association. https://www.usenix.org/conference/soups2019/presentation/faklaris.

[31] M. Fishbein and Icek Ajzen. *Belief, attitude, intention and behaviour: An introduction to theory and research*. Addison-Wesley, Reading, MA, 1975.

[32] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction*, 35(6):456–467, 2019. https://doi.org/10.1080/10447318.2018.1456150.

[33] Veronica Frisancho, Alejandro Herrera, and Silvia Prina. Can a mobile-app-based behavioral intervention teach financial skills to youth? experimental evidence from a financial diaries study. *Journal of Economic Behavior & Organization*, 214:595–614, 2023.

[34] Trevor Gabriel and Steven Furnell. Selecting security champions. *Computer Fraud & Security*, 2011(8):8–12, 2011.

[35] Nina Gerber and Karola Marky. The nerd factor: The potential of S&P adepts to serve as a social

resource in the user's quest for more secure and Privacy-Preserving behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 57–76, Boston, MA, August 2022. USENIX Association. https://www.usenix.org/conference/soups2022/presentation/gerber.

[36] Thomas Groß. Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021:235–258, 2021.

[37] Marco Gutfleisch, Markus Schöps, Stefan Albert Horstmann, Daniel Wichmann, and M Angela Sasse. Security champions without support: Results from a case study with owasp samm in a large-scale e-commerce enterprise. In *Proceedings of the 2023 European Symposium on Usable Security*, pages 260–276, 2023.

[38] Julie M. Haney and Wayne G. Lutters. "it's Scary... It's Confusing... It's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 411–425, Baltimore, MD, August 2018. USENIX Association.

[39] Vagn Lundsgaard Hansen. Popularizing mathematics: from eight to infinity, 2003. https://arxiv.org/abs/math/0305019.

[40] Mark Hassenzahl. The hedonic/pragmatic model of user experience. In Effie Law, Arnold Vermeeren, Marc Hassenzahl, and Mark Blythe, editors, *Towards a UX manifesto. COST294-MAUSE affiliated workshop*, volume 10, pages 10–14, 3rd September 2007, Lancaster, UK, 2007.

[41] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Durmuth, Yixin Zou, and M. Angela Sasse. Digital Security — A Question of Perspective A Large-Scale Telephone Survey with Four At-Risk User Groups . In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 697–716, Los Alamitos, CA, USA, May 2024. IEEE Computer Society.

[42] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. A world full of privacy and security (mis)conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[43] Alice M Isen. Toward understanding the role of affect in cognition. In Jr. R. S. Wyer and T. K. Srull, editors, *Handbook of Social Cognition*, volume 3, pages 179—-236. Lawrence Erlbaum Associates Publishers, 1984.

[44] Allen C Johnston and Merrill Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3):549–566, 2010. https://doi.org/10.2307/25750691.

[45] Noizzie Jutin and Siti Maat. The effectiveness of gamification in teaching and learning mathematics: A systematic literature review. *International Journal of Academic Research in Progressive Education and Development*, 13(1), 02 2024.

[46] Isadora Krsek, Kimi Wenzel, Sauvik Das, Jason I. Hong, and Laura Dabbish. To self-persuade or be persuaded: Examining interventions for users' privacy setting selection. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[47] Oksana Kulyk, Karen Renaud, and Stefan Costica. People want reassurance when making privacy-related decisions—not technicalities. *Journal of Systems and Software*, 200:111620, 2023. https://doi.org/10.1016/j.jss.2023.111620.

[48] Tamara Lopez, Thein Tun, Arosha Bandara, Levine Mark, Bashar Nuseibeh, and Helen Sharp. An anatomy of security conversations in stack overflow. In *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*, pages 31–40. IEEE, 2019.

[49] Sofya Lyakhova and Andrew Neate. Engagement and online mathematics enrichment for secondary students. *Teaching Mathematics and its Applications: An International Journal of the IMA*, 43(3):224–245, September 2024.

[50] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004. https://doi.org/10.1287/isre.1040.0032.

[51] Leonard L Martin, David W Ward, John W Achee, and Robert S Wyer. Mood as input: People have to interpret the motivational implications of their moods. *Journal of Personality and Social Psychology*, 64(3):317—-326, 1993. https://doi.org/10.1037/0022-3514.64.3.317.

[52] John McAlaney and Vladlena Benson. Cybersecurity as a social phenomenon. In Vladlena Benson and John Mcalaney, editors, *Cyber influence and cognitive threats*, pages 1–8. Elsevier, 2020.

[53] U. Menges, J. Hielscher, A. Buckmann, A. Kluge, M. A. Sasse, and I. Verret. Why IT Security Needs Therapy. In S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge, editors, *Lecture Notes in Computer Science. Computer Security. ESORICS 2021 International Workshops Vol. 13106*, page 335–356, 2022. https://doi.org/10.1007/978-3-030-95484-0_20.

[54] Nagham Mohammad, Mihai Nica, Kimberly Levere, and Rachel Okner. Promoting engagement via engaged mathematics labs and supportive learning. *International Electronic Journal of Mathematics Education*, 18(2):em0732, 04 2023.

[55] Norbert Nthala and Ivan Flechais. Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 63–82, Baltimore, MD, August 2018. USENIX Association.

[56] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. Different researchers, different results? analyzing the influence of researcher experience and data type during qualitative analysis of an interview and survey study on security advice. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[57] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 319–338, Santa Clara, CA, August 2019. USENIX Association.

[58] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 1–18, Boston, MA, August 2022. USENIX Association. https://www.usenix.org/conference/soups2022/presentation/pfeffer.

[59] Jakub Przetacznik and Simona Tarpova. Russia's war on Ukraine: Timeline of cyber-attacks. Technical Report March, European Parlament, 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf Accessed 5 April 2023.

[60] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 12 2015.

[61] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS 2012, New York, NY, USA, 2012. Association for Computing Machinery.

[62] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 666–677, New York, NY, USA, 2016. Association for Computing Machinery.

[63] Karen Renaud and Marc Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*, pages 42–56, Costa Rica, 2019. https://doi.org/10.1145/3368860.3368864.

[64] Karen Renaud, Stephen Flowerday, and Karl van der Schyff. Uncertainty in cyber de-responsibilisation. *Computer Fraud & Security*, 2021(8):13–19, 2021. https://doi.org/10.1016/S1361-3723(21)00086-5.

[65] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):1–17, 2021. https://doi.org/10.1057/s41599-021-00746-5.

[66] Tali Sharot. The optimism bias. *Current Biology*, 21(23):R941–R945, 2011. https://doi.org/10.1016/j.cub.2011.10.030.

[67] Kelly Siegel-Stechler and Gretchen Gee. Political and international affairs simulations and college students' civic development. *International Studies Perspectives*, 24(2):115–127, 2023.

[68] Mario Silic and Paul Benjamin Lowry. Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems*, 37(1):129–161, 2020.

[69] SUSAN Squires and MOLLY Shade. People, the weak link in cyber-security: Can ethnography bridge the gap? In *Ethnographic Praxis in Industry Conference Proceedings*, pages 47–57. Wiley Online Library, 2015. https://doi.org/10.1111/1559-8918.2015.01039.

[70] Christine R. Starr. "I'm Not a Science Nerd!": STEM Stereotypes, Identity, and Motivation Among Undergraduate Women. *Psychology of Women Quarterly*, 42(4):489–503, 2018. https://doi.org/10.1177/0361684318793848.

[71] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, 07 2021. https://doi.org/10.2478/popets-2021-0049.

[72] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[73] Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In Serge Gutwirth, Ronald Leenes, and Paul de Hert, editors, *Reforming European Data Protection Law*, pages 333–365. Springer Netherlands, Dordrecht, 2015. https://doi.org/10.1007/978-94-017-9385-8_14.

[74] P. van Schaik, K. Renaud, C. Wilson, J. Jansen, and J. Onibokun. Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, 90:101651, 2020. https://doi.org/10.1016/j.cose.2019.101651.

[75] N Van Yperen, BP Buunk, and J Van der Pligt. Illusoire superioriteit: Het verband met het belang en van de verifieerbaarheid van de vergelijkingsdimensies [illusory superiority: The relation with importance and verifiability of comparison dimensions]. *Fundamentele Sociale Psychologie*, 5:186–200, 1991.

[76] Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. Fear, fun or none: A qualitative quest towards unlocking cybersecurity attitudes. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery.

[77] Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. Beyond fear and frustration - towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 623–642, Philadelphia, PA, August 2024. USENIX Association.

[78] Alexandra von Preuschen, Verena Zimmermann, and Monika Schuhmacher. How do you Feel about Cybersecurity? – A Literature Review on Emotions in Cybersecurity. In Nina Gerber and Verena Zimmermann, editors, *Proceedings of the International Symposium on Technikpsychologie (TecPsy)*. Sciendo, 2023. https://sciendo.com/book/9788366675896.

[79] James Q. Whitman. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, 113(6):1151–1221, 2004.

[80] Corrie Whitmore and Kathryn Schild. Exploring complex concepts through storytelling: A synchronous online health policy course case study and recommendations for implementing across disciplines. *Open Praxis*, 14:242–248, 09 2022.

[81] Brenda K Wiederhold. Increasing cybersecurity through emotional engagement. *Cyberpsychology, Behavior and Social Networking*, 24(9):579–580, 2021. https://doi.org/10.1089/cyber.2021.29224.editorial.

[82] Yuxi Wu, W. Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879, 2022.

[83] Xiaochen Angela Zhang and Jonathan Borden. How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research*, 23(10):1336–1352, 2020. https://doi.org/10.1080/13669877.2019.1646315.

A Survey

Informed Consent for participating in a scientific study on IT security and privacy

Thank you for your interest in our study on IT security and privacy! Before you start, we would like to provide you with some more information: The German Research Association requires explicit consent to voluntarily participating in empirical research. Therefore, we kindly ask you to read the following information on the study, and to confirm the informed consent statement below if you agree to participate. In this study, you will answer some questionnaires and provide some personal information. Completing the study will take approximately 20 minutes. Your participation will be compensated with the amount indicated on the Prolific platform. The collected data (questionnaire responses, demographic information) will only be used for research purposes. Participants in this study will not be exposed to any risk greater than that experienced in everyday life. You can abort the study at any time if you wish without having to provide a reason. All data collected until then will be deleted.

Data protection

The data collection and handling in this study are in accordance with the European General Data Protection Regulation (GDPR) .

The data will only be used for the purposes stated in this informed consent and not be forwarded to a third party for any other purpose. Within this study the following types of data will be collected:
- questionnaire responses, and
- demographic information

As demographic information we will collect:
- gender,
- age (in groups),
- education,
- occupation, and
- experience with IT security and privacy

Confidentiality
The collected data will only be used for research and publication purposes (e.g., a scientific journal) in an aggregated (e.g., as means) and anonymized form. Demographic information such as age and gender do not permit inference to you as a person. At no point in time will we store your name or other definite information.

Data storage
The collected data will be handled by researchers at Technische Universität Darmstadt, Germany. As soon as the research purpose allows it, we will delete all personal data or store it separately from the rest of your answers respectively. Possibly provided personal information will be replaced by a placeholder. The data will be stored in an anonymised form.

Voluntariness & Rights of the Participants
Answering the questions of this study and agreeing to the analysis of your data (especially the collection, storage and publication) is voluntary. You have the right to abort the study any time, to refuse participation, to be informed about the personal data we store and to have the personal data corrected, limited or deleted if you wish. You can revoke the handling of your personal data any time, without this having an influence on the legitimacy on the data analysis done until the moment of revocation. To revoke your agreement please inform the contact person named below verbally or in written form. You also have the right on data portability and the right to complain to a regulator. If you have read and understood the information, and agree to participate in the study, please tick the box next to the agreement below.

I hereby confirm that I have read and understood the information on this study, want to take part in the study and agree to the designated handling of personal data (especially the data collection, storage and publication).
If you have an questions or concerns please contact: [Contact details of the authors]

Survey Items
Please finish the following sentences. Just complete the sentence in the way that comes to your mind first, there are no right or wrong answers. We are interested in your personal associations with this topic.

1. Privacy is a topic that...[text field]
2. It would be so much more fun to protect my (digital) privacy if...[text field]
3. Imagine (digital) privacy was a person, or more precisely, a colleague of yours. Which three character traits would you use to describe him or her? Please use one line per character trait.

text field

text field

text field

1. How would you define privacy? [text field]
2. What is important to you in terms of your privacy? [text field]

1. How well do you protect your privacy compared to...
   Please answer the question only in relation to such people who are in your life, i.e. if you do not have any siblings, please just do not make any statement in relation to your siblings. [Visual analogue scale from 1="less" to 101="more"; randomised order]

   (a) ...your children?

   (b) ...your acquaintances?

   (c) ...your colleagues?

   (d) ...your parents?

   (e) ...your siblings? your partner?

   (f) ...your friends?

Please finish the following sentences. Just complete the sentence in the way that comes to your mind first, there are no right or wrong answers. We are interested in your personal associations with this topic.

1. IT Security is a topic that...[text field]
2. It would be so much more fun to protect my IT security if...[text field]
3. Imagine IT security was a person, or more precisely, a colleague of yours. Which three character traits would you use to describe him or her? Please use one line per character trait.

text field

text field

text field

1. How well do you protect your IT security compared to...
   Please answer the question only in relation to such people who are in your life, i.e. if you do not have any siblings, please just do not make any statement in relation to your siblings. [Visual analogue scale from 1="less" to 101="more"; randomised order]

   (a) ...your children?

   (b) ...your acquaintances?

   (c) ...your colleagues?

   (d) ...your parents?

   (e) ...your siblings?

   (f) ...your partner?

   (g) ...your friends?

1. How often do you talk to other people about IT security and privacy issues?
   (a) I talk to other people about privacy issues...[7-point Likert-like scale from 1="very infrequently" to 7="very frequently"; fallback option="never"]
   (b) I talk to other people about IT security issues...[7-point Likert-like scale from 1="very infrequently" to 7="very frequently"; fallback option="never"]
2. In case you do not talk very frequently to others about privacy: Why don't you talk to other people so often about privacy? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
   (a) Because it is too much effort
   (b) Because I don't want to come across as know-it-all
   (c) Because no one else cares
   (d) Because I do not care
   (e) Because I don't always behave as I would like in this area
   (f) Because I don't want to annoy others
   (g) Because I fear negative reactions
   (h) Because I don't want to be intrusive
   (i) Because there are no opportunities for this to serve as a conversation starter
   (j) Because it is too complicated
   (k) other: [text field]
3. I would talk about privacy much more often with others if....[text field]
4. In case you do not talk very frequently to others about IT security: Why don't you talk to other people so often about IT security? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
   (a) Because it is too much effort
   (b) Because I don't want to come across as know-it-all
   (c) Because no one else cares
   (d) Because I do not care
   (e) Because I don't always behave as I would like in this area
   (f) Because I don't want to annoy others
   (g) Because I fear negative reactions
   (h) Because I don't want to be intrusive
   (i) Because there are no opportunities for this to serve as a conversation starter
   (j) Because it is too complicated
   (k) other: [text field]
5. I would talk about IT security much more often with others if....[text field]
6. It is important you pay attention to the statements. Please agree by choosing "strongly agree". [[7-point Likert scale, 1="strongly disagree", 7="strongly agree"]
   (a) I'm paying attention to the questions in this questionnaire. I confirm this by choosing "strongly agree".
1. I think that someone is paranoid who, in order to protect their own privacy,...[7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order; based on the results from [35]]
   (a) ...uses private mode in browsers.
   (b) ...encrypts their devices.
   (c) ...covers the camera on their (mobile) devices.
   (d) ...uses 2 factor authentication.
   (e) ...only uses messengers that are considered secure.
   (f) ...avoids to use the devices and services of certain providers.
   (g) ...avoids having private data stored on servers that are not subject to strict privacy regulation.
   (h) ...checks attachments before opening them.
   (i) ...uses the tor browser for surfing.
   (j) ...uses complex passwords.
   (k) ...uses tracing blocker.
   (l) ...regularly updates their devices.
   (m) ...does not use social media.
   (n) ...reads privacy policies.
   (o) ...checks links before clicking on them.
   (p) ...locks their devices when they are not using them.
   (q) ...gives as little information as possible on user accounts.
   (r) ...manages permissions on the phone or computer.
   (s) ...uses antivirus programs.
   (t) ...uses VPN.
   (u) ...does not accept optional cookies.
   (v) ...regularly clears their cache.
   (w) ...limits the number of services used.
1. Nerd-Genius scale [70]: What do you think about people who protect their privacy? [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order]
1. How would you rate your general skills in computer security and privacy (e.g., understanding threats, vulnerabilities, and countermeasures)? [single choice; based on [55]]
   (a) Novice
   (b) Competent
   (c) Expert
2. Assuming you believe each of the following to be less competent than you in data security, if they ask you for advice or help with data security, how likely are you to offer it? [7-point Likert-like scale, 1="Very unlikely", 7="Very likely"; randomised order; ; based on [55]]
   (a) Relative
   (b) Friend

(c) Work colleague

(d) Others

3. ATI scale [32] [6-point Likert scale, 1="strongly disagree", 6="strongly agree"; randomised order]
4. SA-6 [30] [5-point Likert scale, 1="strongly disagree", 5="strongly agree"; randomised order]
5. IUIPC-8 [36, 50] [7-point Likert scale, 1="strongly disagree", 7="strongly agree"; randomised order]
6. To confirm that you are paying attention to the questions in the questionnaire, please select the second option from the left on the scale. [7-point Likert scale, 1="strongly disagree", 7="strongly agree"]
   (a) Paying attention to the questions in this questionnaire is important. I agree by choosing the second option from the left of the scale.
7. OPLIS technical scale [73]: In the following you will find different questions about the Internet. Some of the questions are not easy to answer, in order to be able to assess as many people as possible with different levels of knowledge. Therefore, it is not a big deal if you do not know an answer. In that case, simply select "Don't know".

Demographic Information

1. With which gender do you identify most? [single choice]
   (a) female
   (b) male
   (c) other
   (d) prefer not to say
2. How old are you? [single choice]
   (a) 18-20 years
   (b) 21-25 years
   (c) 26-30 years
   (d) 31-35 years
   (e) 36-40 years
   (f) 41-45 years
   (g) 46-50 years
   (h) 51-55 years
   (i) 56-60 years
   (j) 61-65 years
   (k) 66-70 years
   (l) 71-75 years
   (m) 76-80 years
   (n) >80 years
   (o) Prefer not to say
3. What is your highest degree of education? [single choice]
   (a) School student
   (b) High School Diploma
   (c) Bachelor's Degree
   (d) Master's Degree
   (e) Ph.D. or higher
   (f) Other, namely: [text field]
   (g) Prefer not to say
4. What describes your current employment status best? [single choice]
   (a) employed full time
   (b) employed part-time
   (c) unemployed and on the lookout
   (d) unemployed and not on the lookout
   (e) student
   (f) retired
   (g) homemaker
   (h) self-employed
   (i) incapacitated for work
   (j) other:[text field]
   (k) Prefer not to say

Thank you for completing this questionnaire!
We would like to thank you very much for helping us.
Your answers were transmitted. We will now redirect you to Prolific.

B Online Appendix

This article is supplemented by an Online Appendix that provides details on the character traits associated with security and privacy, the codebook, and the statistical analyses results on OSF: https://osf.io/z7hsj/files/osfstorage/68346bfd8ae20e827053930b.

A S&P Associations

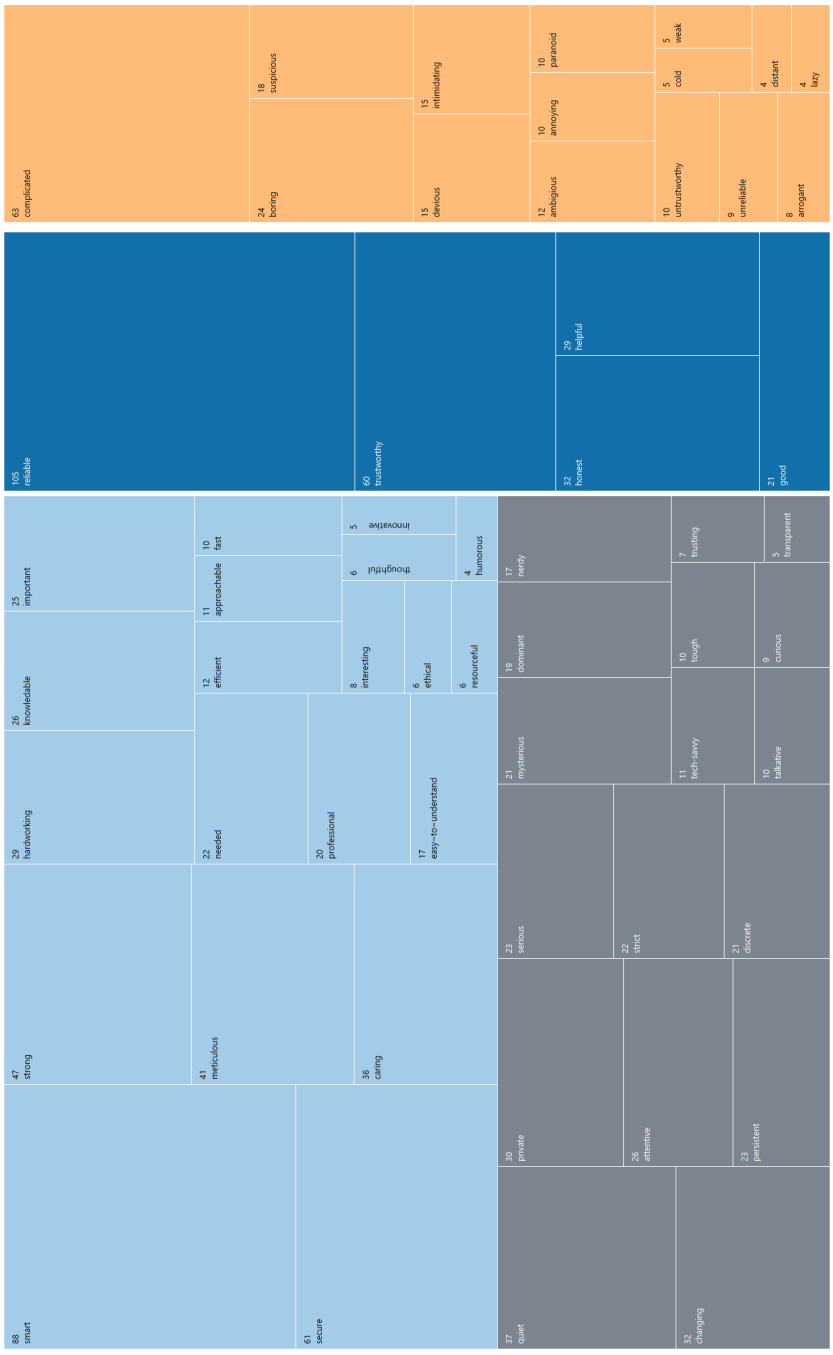


Figure 1: Character traits associated with security. Note: dark blue = very positive, light blue = positive, grey = neutral, orange = negative

Figure 2: Character traits associated with privacy. Note: dark blue = very positive, light blue = positive, grey = neutral, orange = negative

B Codebook

Theme	Code	total count	Example
	I would talk about security much more often with others if....		
Barriers (n = 356)	Knowledge deficit	173 individual: 140 social: 33	individual: "If I was more knowledgeable" (P5), "I knew more about it." (P28) social: "People knew more about it" (P76)
	Disinterest	80 individual: 17 social: 63	individual: "it was a conversation that interested me" (P188) social: "others were interested." (P14)
	Perceived insignificance	53 individual: 22 social: 31	individual: "It was a more obvious problem in my life." (P59); "it were a more relevant topic" (P94) social: "others perceived it as an important issue that affected their lives." (P12)
Normative barriers (n = 50)	"not a common topic"	30	"it came up in daily conversation" (P276),
	common ground	20	"they had the same enthusiasm about the topic." (P136)
Security perceptions (n = 47)	Negative perceptions	33	"It were an easier to understand topic" (P223), "It weren't daunting" (P310)
	Sense of uncontrollability	14	"There was something that could be done" (P77)
Need for facilitators/ triggers (n = 104)	Initiation by others	43	"Others started the conversation first" (P152)
	no media publicity/ public interest	9	"if there were some reason that it was in the news." (P189)
	lack of a trigger	33	"there was a need based on the current state of IT security in the world" (P277)
	need of a suiting environment/ work or class related	19	"It were relevant in the workplace" (359)
	I would talk about privacy much more often with others if....		
Barriers (n = 305)	Knowledge deficit	90 individual: 64 social: 26	individual: "I understood it better" (P322) social: "Other people were better informed" (P380)
	Disinterest	84 individual: 13 social: 65	individual: "it were interesting" (P100) social: "it was something of interest to them" (P166)
	Perceived insignificance	51 individual: 25 social: 26	individual: "it was important to me" (P248) social: "they can see the value in protecting personal privacy." (P232)
Normative barriers (n = 80)	"not a common topic"	47	"It were a typical topic of conversation" (P333)
	interpersonal lack of trust	6	"I knew I could trust them" (P382)
	lack of social acceptance of the topic	27	"people were more open to the topic." (P99)
Privacy perceptions (n = 48)	Negative perceptions	30	"It were not such a depressing conversation piece" (P145)
	Sense of uncontrollability	18	"it were possible to achieve." (P173)
Need for facilitators/ triggers (n = 127)	Initiation by others	67	"others talked about it with me" (P225)
	no media publicity/ public interest	12	"there were more public interest in it." (P243)
	lack of a trigger	41	"It happens to my friend as a problem" (P224)
	need of a suiting environment	7	"I was in a computer program or class" (P29)
	Security is a topic that…		
Knowledge and Experience Gaps (n = 83)			"I don't know much about" (P110), "is relatively foreign to me." (P260), "I know very little about" (P364)
Positive Perceptions (n = 166)	interesting	22	"sounds interesting" (P41)
	relevant/ important	144	"Is important in today's world." (P1), "is very important and should be taken seriously." (P143)
Negative Perceptions (n = 98)	boring/ annoying	17	"bores me" (P22), "security is a topic I am sick of hearing about" (P192)
	scary/ left alone/ concern/ worrysome	24	"sounds scary" (P159), "invokes fear and concern" (P417)
	complex/ overwhelmed/ confused	57	"Is very complicated and multilayered." (P187)
Non-valenced perceptions/ associations (n = 31)	fast changing	11	"is constantly developing." (P47)
	is work-related	20	"Comes up daily in my job" (P348)

Theme	Code	Total Count	Example
Demand for increased Importance and Attention (n = 63)	should be talked about more often	22	"needs to be discussed more often" (P149)
	should be taken more seriously	41	"does not receive enough respect." (P345)
definitions (n = 20)			"involves the protection of any kind of technology and information" (P132)
	Privacy is a topic that…		
Positive Perceptions (n = 237)	is important/I care about/take seriously	226	"is very important to me." (P211)
	is interesting	11	"Privacy is a topic that I am very interested in" (P208)
Negative Perceptions (n = 94)	lack of interest	11	"bores me" (P398)
	controversial/sensitive/ is interpreted differently	31	"that can be gauged in different ways by different people" (P26), "is controversial" (P18)
	complex/ difficult to understand	16	"is more complicated than it might seem." (P435)
	concern/ worry/evokes negative feelings	36	"worries me." (P233), "is stressful" (P174)
Non-valenced perceptions/ associations (n = 37)	public interest/ passion (but is not necessarily perceived as important/necessary)	37	" is a pretty hot topic right now" (P276), "a lot of people are talking about these days" (P276)
Demand for increased importance and Attention (n = 91)	should be talked about more often or often overlooked; perceived lack of significance (others)	27	"is overlooked by far too many" (P453)
	should be taken more seriously/ is not taken seriously	64	"isn't taken as seriously as it needs to be." (P218)
definition (n = 24)			"that talks about the protection of information" (P294)
	It would be so much more fun to protect my IT security if…		
Empowerment through Education (n = 89)	knowledge	89	"if I learned more about it" (P5)
Motivation and Engagement (n = 180)	incentives	27	"got cake every month there were no breaches" (P317)
	complexity	116	"It was easier to understand what it is" (P63)
	decreasement fear/ negative connotation	21	"there was not a negative connotation" (P159)
	less boring/ more interest/ intrapersonal enrichment (e.g., fun to learn)	16	"It wasn't so boring" (P11)
Ease of use and Accessibility (n = 74)	exclusion of barriers/ make it userfriendly	21	"My work didn't block links needs for work." (P279)
	(monetary) affordability	20	"If I didnt have to pay for it" (P130)
	perceived control	33	"I could choose what to share, or how it was shared." (P61)
Enablement and Responsibility (n = 75)	automatic/ effortless	29	"I didn't have to do anything to protect it." (P265)
	external responsibility	20	"government and internet providers did more to secure the internet." (P473)
	increasement perceived validity/ perceived effectiveness	26	"it felt possible to actually do so" (P191)
Not-fun (n = 28)	serious matter	8	"it weren't so serious and potential losses weren't so great." (P475)
	not a fun topic	20	"I don't see this as fun" (P28)
	It would be so much more fun to protect my IT privacy if…		
Empowerment through Education (n = 35)	knowledge	35	"I knew more about it" (P44)
Motivation and Engagement (n = 184)	incentives	30	"There was a financial incentive." (P206)
	complexity	103	"it wasn't so complicated" (P8)
	decreasement fear/ negative connotation	24	"it was less scary to think about" (P55)
	less boring/ more interest/ intrapersonal enrichment (e.g., fun to learn)	27	"it was gamified in some way" (P78)

Table 2: Codebook Table - Part 2

Theme	Code	total count	Example
Ease of use and Accessibility (n = 99)	exclusion of barriers/ make it userfriendly	20	"was not such hard work" (P458)
	(monetary) affordability	20	"if it was free or inexpensive." (P20)
	user friendly	13	"it were portrayed in a clear and entertaining manner" (P90)
	perceived control	46	"could control what others see when I'm online." (P375)
Enablement and Responsibility (n = 111)	automatic/ effortless	31	"if it happend automatically" (P211)
	external responsibility	29	"there is better transparency from companies that claim to protect my privacy." (P117)
	increasement perceived validity/ perceived effectiveness	51	"there was tangible proof that all my efforts kept my data secure" (P467)
Not-fun (n = 27)	serious matter	16	"it weren't such a serious matter" (P30)
	not a fun topic	11	"I dont think this is a "fun" topic" (P141)
How would you define privacy?			
keeping information private (n = 221)			"Privacy is the act of keeping things confidential and protected either physically, mentally, and emotionally and can take place in so many aspects of our lives" (P66), "To keep things to oneself" (P329)
control (n = 105)			"Privacy is that I get to define how much of my personal life, choices, actions, behaviours, and attitudes I share with others." (P150), "Privacy is retaining control over the amount and type of information that I share." (P82), "Privacy is a choice. Its up to you if you want someone to know something about you or not." (P82)
protected (n = 91)			"Privacy is safeguarding data, personal identifying information, and use of technology information from those who may try to hack my information or steal my identity. It also guards against who uses my data and in what ways." (P490), "The level at which your personal information is protected" (P9)
right (n = 56)			"Privacy is the right to keep your business your business." (P131), "the right to choose your own boundaries around personal information" (P205)
left alone (n = 48)			"you need to be kept from other people." (P325)
unobserved (n = 44)			"The ability to exist without being monitored" (P96), "ability to not be heard/seen/listen" (P48)

Table 3: Codebook Table - Part 3

C Statistical Analyses Results

	Estimator	SD	df	T	Sig.	95% CI	
						Lower	Upper
Intercept	72.72	5.37	437.00	13.54	<.001*	62.17	83.28
Skill							
Novice	-20.27	5.93	437.00	-3.42	.001*	-31.93	-8.61
Competent	-13.95	5.64	437.00	-2.47	.014*	-25.04	-2.86
Expert							
Target	/	/	/	/	/	/	/
Friends	6.04	6.65	818.86	0.91	.364	-7.01	19.09
Parents	11.69	7.65	889.99	1.53	.127	-3.32	26.70
Siblings	6.91	7.14	866.72	0.97	.333	-7.10	20.91
Children	9.42	7.70	812.80	1.22	.222	-5.70	24.54
Acquaintances	6.91	6.72	834.03	1.03	.305	-6.29	20.11
Colleagues	-0.26	6.86	850.33	-0.04	.970	-13.72	13.21
Partner	/	/	/	/	/	/	/
*Skill*Target*							
Friends*Novice	5.10	7.31	813.43	0.70	.486	-9.26	19.45
Parents*Novice	-0.06	8.42	889.92	-0.01	.994	-16.59	16.47
Siblings*Novice	1.62	7.87	865.72	0.21	.837	-13.82	17.06
Children*Novice	-1.26	8.51	812.70	-0.15	.882	-17.97	15.44
Acquaintances*Novice	7.28	7.40	828.51	0.98	.325	-7.24	21.79
Colleagues*Novice	9.06	7.56	847.27	1.20	.231	-5.77	23.89
Partner*Novice	/	/	/	/	/	/	/
Friends*Competent	2.69	6.98	817.58	0.39	.700	-11.00	16.39
Parents*Competent	0.16	8.03	889.98	0.02	.984	-15.60	15.93
Siblings*Competent	-0.46	7.50	867.16	-0.06	.951	-15.18	14.27
Children*Competent	-5.31	8.11	812.10	-0.65	.513	-21.24	10.61
Acquaintances*Competent	5.00	7.06	832.85	0.71	.479	-8.86	18.85
Colleagues*Competent	9.76	7.21	849.79	1.35	.176	-4.38	23.90
Partner*Competent	/	/	/	/	/	/	/

Table 4: Mixed-effects model of skill level and comparison target on perceived privacy protection.

	Estimator	SD	df	T	Sig.	95% CI	
						Lower	Upper
Intercept	82.21	5.12	426.00	16.06	<.001*	72.14	92.27
Skill							
Novice	-28.88	5.67	426.00	-5.09	<.001*	-40.04	-17.73
Competent	-20.02	5.38	426.00	-3.72	<.001*	-30.61	-9.44
Expert	/	/	/	/	/	/	/
Target							
Friends	2.79	6.52	836.82	0.43	.668	-10.00	15.59
Parents	7.45	7.21	869.21	1.03	.302	-6.69	21.59
Siblings	4.03	6.85	854.87	0.59	.557	-9.41	17.46
Children	0.02	7.52	783.61	0.00	.998	-14.75	14.78
Acquaintances	2.63	6.52	834.89	0.40	.687	-10.17	15.43
Colleagues	-4.57	6.49	822.76	-0.70	.481	-17.31	8.17
Partner	/	/	/	/	/	/	/
*Skill*Target*							
Friends*Novice	1.22	7.19	830.95	0.17	.865	-12.89	15.33
Parents*Novice	6.00	7.96	868.81	0.75	.452	-9.63	21.62
Siblings*Novice	0.16	7.56	853.20	0.02	.983	-14.69	15.00
Children*Novice	4.80	8.34	783.40	0.58	.565	-11.57	21.17
Acquaintances*Novice	4.60	7.19	829.61	0.64	.523	-9.52	18.72
Colleagues*Novice	6.78	7.17	819.10	0.95	.345	-7.29	20.86
Partner*Novice	/	/	/	/	/	/	/
Friends*Competent	1.77	6.85	835.19	0.26	.796	-11.67	15.21
Parents*Competent	3.49	7.57	869.14	0.46	.645	-11.38	18.35
Siblings*Competent	-0.86	7.20	855.09	-0.12	.905	-15.00	13.28
Children*Competent	2.99	7.93	782.61	0.38	.707	-12.58	18.55
Acquaintances*Competent	4.54	6.85	833.49	0.66	.507	-8.90	17.99
Colleagues*Competent	6.69	6.82	822.04	0.98	.327	-6.70	20.08
Partner*Competent	/	/	/	/	/	/	/

Table 5: Mixed-effects model of skill level and comparison target on perceived security protection.

Comparisons	M	SD	95% CI of Difference		T	df	Sig.	Bonferroni-Holm adjusted α	d
			Lower	Upper					
parents - partner	11.735	31.626	8.683	14.787	7.559	414	<.001*	.002	0.371
acquaintances - partner	11.751	33.784	8.574	14.927	7.271	436	<.001*	.003	0.348
friends - partner	9.670	29.093	6.935	12.406	6.949	436	<.001*	.003	0.332
colleagues - partner	8.690	35.405	5.330	12.050	5.084	428	<.001*	.003	0.245
siblings - partner	6.629	29.475	3.768	9.491	4.554	409	<.001*	.003	0.225
acquaintances - colleagues	3.895	20.590	2.041	5.749	4.127	475	<.001*	.003	0.189
siblings - acquaintances	-5.310	28.822	-7.986	-2.634	-3.900	447	<.001*	.003	0.184
children - partner	6.312	31.475	3.073	9.552	3.831	364	<.001*	.004	0.201
parents - siblings	4.679	26.521	2.165	7.193	3.659	429	<.001*	.004	0.176
children - acquaintances	-5.771	35.090	-9.292	-2.250	-3.223	383	.001*	.004	0.164
friends - acquaintances	-3.037	20.973	-4.898	-1.175	-3.205	489	.001*	.005	0.145
parents - children	5.371	32.226	2.036	8.707	3.167	360	.002*	.005	0.167
friends - siblings	2.473	24.293	0.218	4.729	2.155	447	.032	.006	-
friends - children	3.240	30.974	0.132	6.347	2.050	383	.041	.006	-
parents - colleagues	2.924	34.835	-0.307	6.155	1.779	448	.076	.007	-
friends - parents	-2.258	28.871	-4.921	0.405	-1.666	453	.096	.008	-
children - colleagues	-2.072	35.407	-5.662	1.519	-1.135	375	.257	.010	-
siblings - colleagues	-1.329	30.687	-4.211	1.553	-0.906	437	.365	.013	-
siblings - children	1.392	29.581	-1.665	4.450	0.895	361	.371	.017	-
friends - colleagues	0.781	22.687	-1.264	2.827	0.750	474	.453	.025	-
parents - acquaintances	-0.615	32.525	-3.612	2.381	-0.404	454	.687	.050	-

Table 6: Paired samples t-tests on perceived level of privacy protection per comparison target.

Comparisons	M	SD	95% CI of Difference		T	df	Sig.	Bonferroni-Holm adjusted α	d
			Lower	Upper					
parents - partner	11.623	28.696	8.806	14.441	8.111	400	<.001*	.002	0.405
parents - siblings	8.075	24.674	5.725	10.425	6.755	425	<.001*	.003	0.327
acquaintances - colleagues	5.422	17.517	3.829	7.015	6.689	466	<.001*	.003	0.310
parents - colleagues	9.899	30.901	6.994	12.805	6.697	436	<.001*	.003	0.320
friends - parents	-6.800	27.135	-9.326	-4.275	-5.293	445	<.001*	.003	0.251
acquaintances - partner	6.819	31.445	3.821	9.817	4.470	424	<.001*	.003	0.217
parents - children	7.138	29.888	3.987	10.289	4.455	347	<.001*	.003	0.239
friends - partner	4.799	27.039	2.230	7.368	3.672	427	<.001*	.004	0.177
parents - acquaintances	4.502	28.126	1.879	7.126	3.373	443	.001*	.004	0.160
friends - colleagues	3.019	20.126	1.191	4.847	3.245	467	.001*	.004	0.150
friends - acquaintances	-2.493	17.415	-4.050	-0.936	-3.146	482	.002*	.005	0.143
siblings - acquaintances	-3.718	25.948	-6.141	-1.295	-3.016	442	.003*	.005	0.143
children - partner	4.100	28.890	1.102	7.099	2.689	358	.007	.006	-
siblings - partner	3.465	26.917	0.819	6.111	2.575	399	.010	.006	-
children - acquaintances	-3.210	33.853	-6.661	0.242	-1.829	371	.068	.007	-
friends - siblings	1.389	23.070	-0.755	3.534	1.273	446	.204	.008	-
children - colleagues	2.038	33.736	-1.429	5.506	1.156	365	.248	.010	-
siblings - colleagues	1.429	27.384	-1.155	4.012	1.087	433	.278	.013	-
colleagues - partner	1.508	32.284	-1.584	4.601	0.959	420	.338	.017	-
friends - children	1.059	31.207	-2.110	4.227	0.657	374	.512	.025	-
siblings - children	-0.047	28.575	-3.013	2.919	-0.031	358	.975	.050	-

Table 7: Paired samples t-tests on perceived level of security protection per comparison target.

Comparison a - b	Mean Rank$_a$	Mean Rank$_b$	Z-value	Sig.	Bonferroni-Holm adjusted α	r
Novice - Competent	183.61	259.09	-5.991	<.001*	.017	0.278
Novice - Expert	85.39	142.50	-5.434	<.001*	.025	0.396
Competent - Expert	165.06	215.13	-2.900	.004*	.050	0.158

Table 8: Wilcoxon ranked-sum tests on privacy literacy measured via OPLIS for different self-assessed skill levels.

Comparisons	M	SD	95% CI of Difference		T	df	Sig.	Bonferroni-Holm adjusted α	d
			Lower	Upper					
Novice - Competent	-0.74	0.09	-0.91	-0.57	-8.57	285.284	<.001*	0.017	-0.872
Novice - Expert	-1.67	0.14	-1.95	-1.39	-12.02	54.221	<.001*	0.025	-1.888
Competent - Expert	-0.92	0.15	-1.23	-0.62	-6.02	336	<.001*	0.050	-1.151

Table 9: Independent samples t-tests on security attitude measured via SA-6 for different self-assessed skill levels.

Comparisons	M	SD	95% CI of Difference		T	df	Sig.	Bonferroni-Holm adjusted α	d
			Lower	Upper					
Novice - Expert	-1.75	0.33	-2.40	-1.09	-5.27	165.00	<.001*	.017	-1.063
Competent - Expert	-1.26	0.33	-1.91	-0.62	-3.85	324.00	<.001*	.025	-0.739
Novice - Competent	-0.48	0.17	-0.83	-0.14	-2.78	431.00	.006*	.050	-0.287

Table 10: Independent samples t-tests on frequency of privacy conversations for different self-assessed skill levels.

Comparisons	M	SD	95% CI of Difference		T	df	Sig.	Bonferroni-Holm adjusted α	d
			Lower	Upper					
Novice - Competent	-0.75	0.17	-1.09	-0.41	-4.39	403.00	<.001*	.017	-0.48
Novice - Expert	-2.73	0.32	-3.37	-2.09	-8.43	148.00	<.001*	.025	-1.72
Competent - Expert	-1.98	0.31	-2.59	-1.37	-6.41	313.00	<.001*	.050	-1.23

Table 11: Independent samples t-tests on frequency of security conversations for different self-assessed skill levels.

Chapter 5

Paper C: Exploration and Improvement of Attitudes Towards Organizational Cybersecurity

The paper was published as follows:

Alexandra von Preuschen, Carolin Benda, Monika C. Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3706598.3713538

Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes

Alexandra von Preuschen
Justus Liebig University Giessen
Giessen, Germany
alexandra.vonpreuschen@wirtschaft.uni-giessen.de

Carolin Benda
Justus Liebig University Giessen
Giessen, Germany
carolin.benda@gmail.com

Monika Christine Schuhmacher
Justus Liebig University Giessen
Giessen, Germany
monika.schuhmacher@wirtschaft.uni-giessen.de

Verena Zimmermann
Department of Humanities, Social and Political Sciences
ETH Zurich
Zurich, Switzerland
verena.zimmermann@gess.ethz.ch

Abstract

Employees, once seen as the weakest link in organizational cybersecurity, are now recognized as crucial defenders against malicious attacks. Thus, understanding employee attitudes towards cybersecurity, a major factor driving security behavior, is essential for protecting organizations. Using semi-structured interviews and focus groups, this study holistically explores attitudes toward cybersecurity, its influencing factors, and the employees' needs for fostering positive attitudes. The study offers in-depth insights into affective, cognitive, and behavioral components of attitudes, ranging from annoyance and fear to appreciation for cybersecurity measures. Influencing key factors include (in)direct cybersecurity experiences and individual perceptions - both highlighting social influences. For developing positive attitudes, employees express needs related to the company's social and cultural framework, communication styles, educational contents and formats. The study contributes to developing effective security strategies that address the individual, social, and organizational factors that shape cybersecurity attitudes, ultimately promoting a stronger organizational security.

CCS Concepts

• **Security and privacy** → **Human and societal aspects of security and privacy**; Social aspects of security and privacy; • **Human-centered computing** → *Empirical studies in HCI*.

Keywords

Attitude, Cybersecurity, Interview, Focus Group, Organization, Employee

ACM Reference Format:
Alexandra von Preuschen, Carolin Benda, Monika Christine Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3706598.3713538

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713538

1 Introduction

Given the increasing prevalence of phishing attacks driven by emerging technologies like Generative AI [12, 53], it is more critical than ever for organizations to strengthen their cybersecurity strategies by incorporating both technological and human factors. In recent years, employees have increasingly been recognized as a crucial part of the solution - the first line of defense [108]. Thus, understanding factors that drive employees' cybersecurity behavior is crucial for protecting organizations from the success of malicious attacks. Behavioral research has shown that attitudes are a major contributor to behavior [4]. Various studies confirm the significant impact of attitudes in cybersecurity: On the one hand, positive attitudes can lead to positive cybersecurity behaviors and adherence to security policies; On the other hand, negative attitudes may result in negligence and rather unfavorable behavioral tendencies [54, 89]. Notably, a study by de Kok et al. [30] demonstrates that the affective component of attitudes (how employees feel about cybersecurity) is even more important than the cognitive one (how they perceive and evaluate cybersecurity) in explaining subsequent behavior, displaying the necessity to explore cybersecurity attitudes holistically in order to ultimately promote positive cybersecurity behavior in organizations.

Recognizing the general importance of attitudes in cybersecurity, organizations implement various strategies to foster cybersecurity attitudes that ultimately encourage secure behaviors. The three most common approaches are:

(1) Modifying cognitive attitudes encompassing evaluations (e.g., importance ratings) by employing *fear* appeals to emphasize the potential consequences of non-compliance [16, 35, 57, 78],
(2) Stimulate positive affective attitudes by making cybersecurity "*fun*" often involving gamification to make the topic more enjoyable and interactive [11, 88], or
(3) *No* attitude appeal, taking a more traditional approach that focuses purely on factual knowledge transfer [35].

Few methods, however, extend beyond these strategies, combine them, or assess their impact on attitudes. Therefore, exploring

the needs that foster positive attitudes could be key to improving cybersecurity behavior.

Yet, organizational cybersecurity is a social topic involving collective behaviors and interactions of employees [79, 105]. This presents unique challenges that need to be addressed in research accordingly. Similarly, attitude research shows that attitudes are fundamentally social, as they are shaped, influenced and changed by reciprocal interactions with the surrounding social context [19, 72], underscoring the importance of exploring attitudes from a social perspective.

Building on prior research exploring cybersecurity attitudes including studies that have developed multiple approaches to measuring and investigating their impact on cybersecurity behavior [20, 30, 32, 41, 70], we provide and complement previous work with a comprehensive examination of attitudes as a multifaceted concept that is socially constructed.

Consequently, this study aims to understand employee attitudes towards cybersecurity, the factors influencing these attitudes while minding its social nature, and employees' needs for fostering positive attitudes within organizations. Ultimately, we give recommendations on how to foster positive cybersecurity attitudes. Thus, the research questions (RQs) are:

- RQ1: What are employees' attitudes towards cybersecurity?
- RQ2: Which factors influence employees' attitudes towards cybersecurity?
- RQ3: What are the employees' needs for positive cybersecurity attitudes (and, ultimately, positive cybersecurity behavior)?

To tackle these research questions, the study utilized a qualitative approach, employing semi-structured interviews with employees from various departments (N = 17) and four focus groups with the very same participants, encompassing a brainstorming and joint working task to obtain in-depth insights. The findings of the study provide valuable insights into the multifaceted nature of cybersecurity attitudes, shedding light on the key factors that influence these attitudes, and the specific needs that must be addressed to promote positive cybersecurity attitudes. The contributions of the study are manifold:

- First, we offer detailed insights into cybersecurity attitudes as a multifaceted concept and how they are shaped within organizational settings.
- Second, we identify several needs that must be addressed to foster positive cybersecurity attitudes. For instance, needs concerning the social and cultural framework of the organization or the communication style of security-related content.
- Third, building on the findings, we provide practical recommendations for implementing human-centered cybersecurity strategies fostering positive cybersecurity attitudes such as viewing security as a process or implementing a positive mindset.
- Fourth, we demonstrate that cybersecurity strategies need to go beyond fear, fun or none, encompassing social factors and self-reflection.

2 Related Work

We first define attitudes and related conceptualizations. Subsequently, the literature on attitudes in cybersecurity is presented.

2.1 Perspectives on Attitudes

Allport [7] describes attitudes as a psychological and neurological state of preparedness, shaped by experience, which influences an individual's responses to related objects and situations. Here, the stable and enduring nature of attitudes are emphasized, which are regarded as a summary of evaluations stored within an individual's mind and retrieved to form a response when exposed to the attitude's object [63].

Other approaches suggest that the mind rather activates associations, and that such associations activate evaluations when faced with an attitude's object [63] or they stress attitude's role in making sense of the individual's environment. Thus, these approaches see their origin in past experiences, social processes, and contextual factors [93]. Although the definitions of attitudes significantly differ, the evaluative characteristic of attitudes is often emphasized in the literature. For example, Ajzen [3] characterizes attitudes as an individual's tendency to react positively or negatively towards an object, person, institution, event, or any other distinguishable element of their environment [4]. The tripartite model of attitude extends previous approaches by proposing a structure encompassing an affective, cognitive, and conative component allowing for potentially conflicting components [5, 6, 107]:

(1) The *affective* component of attitude describes emotional reactions [1, 91]. An emotional reaction might include feelings such as admiration or disgust, or a sense of appreciation or disapproval. An example of the affective component is the fear of making mistakes when approaching a new cybersecurity measure. While the affective component of attitudes remains relatively stable as an evaluative predisposition, emotions are rather intense and short-lived [1, 55, 91].
(2) The *cognitive* component of attitude refers to the role of cognition in an individual's attitude, including their beliefs and thoughts about, among other things, an object, event, or institution [1, 91]. Beliefs that cybersecurity training does not prevent social engineering attacks is an example of a negative, cognitive component of attitude. While a set of beliefs is sometimes referred to as a mental model [69], mental models are rather described as relatively dynamic, systemic representations of reality [56]. This flexibility distinguishes them from the relatively stable, evaluative judgments about specific objects in the cognitive component of attitudes [4, 63, 63]. However, since the definitions of these concepts are often not clearly distinguished, we also consider the literature on mental models.
(3) The *conative* component of attitude concerns behavioral inclinations, intentions, commitments, or actions in respect of an object, event, or institution. Behavioral attitudes can be investigated by considering what individuals say, plan to, or would do with regard to the object in question [6]. For instance, that one wishes to refuse to participate in supplemental cybersecurity training could be interpreted as a negative conative component of attitude.

While attitudes are recognized as a key factor in explaining behavior, actions are more accurately understood as resulting from an interaction between attitudes and various influences—such as environmental factors, situational contexts, and individual differences - such as social norms as outlined in the theory of planned behavior [6]. The tripartite model of attitudes does not conflict with these theories, despite incorporating a behavioral component. Rather than seeing affect and cognition as direct predictors of behavior, the model integrates three interacting components at one level [3]. Thus, the conative component does not directly predict specific behavioral outcomes of attitudes but rather represents a predisposition toward behavior [107] based on observed prior actions and verbal statements about future intentions [19].

2.2 Attitudes in Cybersecurity

Many studies investigated the impact of attitudes, such as consumer attitudes towards privacy and security in the adoption of internet of things-devices, fitness trackers, mental health applications [43, 45, 59, 62], or user data sharing across online services and companies [14].

Researchers have observed positive effects of attitudes towards the intention of using anti-spyware or overall compliance [20, 31, 52]. In general, prominent theories in cybersecurity research, like the theory of planned behavior and the knowledge-attitude-behavior model, emphasize attitudes as a key factor in predicting cybersecurity intentions and behaviors [20, 48, 52, 70, 83]. Concerning the effect of the different components of attitudes on behavior, de Kok et al. [30] demonstrated that, both affective and cognitive components, positively influence intention to adopt cybersecure behavior, with the affective component having a greater impact than the cognitive aspect.

This highlights the critical need to explore cybersecurity attitudes within organizations, as they play a fundamental role in shaping both individual and collective security practices.

Components of Cybersecurity Attitudes. Only a few studies investigate cybersecurity attitudes in detail or holistically, and none implement the tripartite model of attitudes. Yet, some articles explore related constructs such as emotions, mental models, or only investigate cybersecurity attitudes in specific areas of cybersecurity [9, 38, 51, 80, 97, 100]. For instance, Da Silva et al. revealed that cybersecurity is often considered as *mystical, unknown and fearful to the uninitiated* [25, p.1]. Similarly, for a specific context, Wu and Zappala revealed that encryption for personal communication is often viewed negatively, suggesting sensitivity indicates an illegal activity or undue worry [104]. In line with that, Renaud et al. [80] explored cybersecurity perceptions also finding that cybersecurity is more often associated with negative attributes such as fear or complexity rather than positive aspects even though many participants agreed on cybersecurity being important. This research highlights the relevance in particular of the affective and cognitive component of attitudes.

In contrast, measurement tools of attitudes towards cybersecurity encompass a spectrum of factors, primarily focusing on the cognitive and conative component: The Security Attitude inventory SA-13, highlights key dimensions of attitudes such as engagement with security measures, attentiveness to security measures, resistance to security measures, and concernedness with improving compliance, showing associations with the conative component of attitude, e.g., with security behavior intention or recent behaviors [39]. Further attitude measurement tools including the SA-13 (SA-6) [39, 41], the sub-scale on attitudes towards choosing passwords in the Security Behavior Intentions Scale (SeBIS) and the attitude scale within the questionnaire of human aspects of information security-questionnaire (HAISQ) [70] mostly measure conative attitudes, i.e., behavioral tendencies or cognitive attitudes, i.e., evaluations of cybersecurity behavior or competencies. Despite the availability of measurement tools, there is a noticeable gap in research exploring the full range of components that shape cybersecurity attitudes particularly in integrating the affective component. Existing approaches tend to emphasize conative and cognitive dimensions, overlooking attitudes' complex and social nature. Examining attitudes through the lens of the tripartite model provides a holistic understanding of the construct, offering valuable insights into potential discrepancies among its components.

Impacting Factors on Cybersecurity Attitudes. Several studies investigate attitudes toward specific areas of cybersecurity. Arnold et al. [9] find that the introduction of multi-factor authentication resulted in negative emotions and at the same time did not result in a higher feeling of security. Furthermore, Fagan et al. [38] show that software update messages not only resulted in negative feelings i.e. affective component, but also negative beliefs, i.e. cognitive component. Additionally, when security measures interfere with daily tasks, it tends to create negative attitudes [50]. Concerning cybersecurity as a concept, individual factors such as knowledge or awareness level have been found as major predictors of attitudes [70, 82]. Finally, research has investigated security breach concern level, response cost, self-efficacy and experiences as impacting factors for cybersecurity attitudes [50, 83].

Beyond individual factors, social factors are highly relevant for the formation of attitudes [90]. The security of an organization depends not only on individual actions but also on how employees collaborate, perceive others' cybersecurity practices, and how they anticipate being perceived as a consequence of their cybersecurity behavior. Teams often need to make joint decisions regarding security measures, and a shared commitment to cybersecurity can significantly enhance the organization's overall security [105]. For example, Wang et al. [99] demonstrated that the practice of account-sharing among team members is based on social needs that may conflict with technical security requirements. In line with that, recent work shows that social perceptions, peer influences, and group dynamics play crucial roles in shaping individual emotions and behaviors towards cybersecurity [97]. Specifically, prior research has shown that social factors, such as norms and involvement, significantly influence cybersecurity attitudes [54] and highlighted the impacts of life experiences and collective mental models on individual perceptions [58, 83, 95]. Not only peer influence, but even non-personal social influence can impact on users security and privacy decisions [61]. Further, Menges et al. [65] conducted a survey on the perceptions of, and emotions towards, IT staff and revealed a dysfunctional relationship between employees and IT staff based on negative attitudes expressed in the communication.

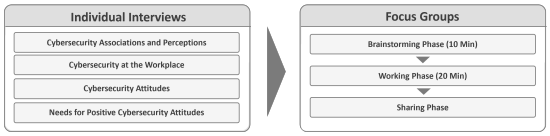


Figure 1: Depiction of the study procedure

We argue that measures to foster positive attitudes toward cybersecurity, which are developed within teams, are accepted by team members and are thus more likely to be effective and stable over time, similar to positive effects of training programs created collectively [23]. While initial research has begun to identify factors shaping cybersecurity attitudes, no study to date has thoroughly investigated these influencing factors in a strategic and holistic manner, especially within the organizational context. Further, despite the recognized positive effects of attitudes on cybersecurity behavior, no research has yet identified the needs for fostering positive attitudes.

3 Methods

The following sections describe the research design, the interview and focus group structure, the sample, accompanying ethical considerations, and the data analysis approach.

3.1 Research Design

This study followed a two-step research design including in-depth individual interviews and focus groups. Individual interviews facilitated the collection of detailed personal insights into participants' attitudes, providing a nuanced understanding of their complexities. Focus groups, on the other hand, provided a collaborative environment for discussing how attitudes about cybersecurity are influenced and shaped within a group dynamic, reflecting the social nature of organizational cybersecurity. The procedure is depicted in Figure 1.

Individual Interviews. In the first step, semi-structured interviews with all participants were conducted individually. First, the interviewees were asked about their associations with the term "cybersecurity". Following a brief definition of cybersecurity, the interviewees were asked about their perceptions of cybersecurity in their working routines, their attitudes toward cybersecurity, and the origins of their respective attitudes. Moreover, the interviewees were asked to describe how they prioritized cybersecurity in their daily work. Then, interviewees were asked to report whether they felt as though their attitudes influence their cybersecurity-related behaviors. The interviewees were also asked to describe how they incorporated cybersecurity measures into their daily work routines. Before concluding, participants were asked for their recommendations on designing cybersecurity measures to foster positive attitudes toward cybersecurity. All interviews were conducted via video call and subsequently transcribed.

Focus Groups. In the second step, focus groups were formed with the same participants based on their departmental affiliation. Before the focus groups, one group member was elected group speaker and edited the slide during the group discussion. As a warm-up, each group was asked to create a group name, which also aimed to enhance and strengthen existing group coherence.

In an interactive setting, focus group members were first asked to brainstorm about factors improving cybersecurity attitudes and then visualize a model, chart, or overview of their results. For the respective assignments, the participants had 10 min and 20 min, respectively. They were provided with a Microsoft PowerPoint slide to outline their results for both the brainstorming and working phase. This slide deck template included two supporting slides with icons (icon box) and tools (toolbox) for editing. During the brainstorming phase, participants were provided with the "toolbox" slide, which contained basic visual elements such as arrows, shapes, and text boxes to help participants structure their ideas and thoughts. Here, participants could reflect freely without being biased by predefined categories or concepts. The slide encompassing the "icon box" was presented immediately after the brainstorming phase to help participants quickly visualize their results. To further mitigate potential bias, participants were informed that the icons were optional and that they were free to include their own symbols or visual elements (see Figure 2). After both phases, the brainstorming and working phase, the groups presented their results. We decided to transcribe only the presentation of the results to allow participants to discuss and develop their ideas freely without the pressure of being recorded. This approach fostered an open and creative environment.

3.2 Participants

A total of seventeen employees from a media agency participated in this study, selected through purposive sampling to capture a diverse range of perspectives on cybersecurity. The agency operates in multiple countries and has over 1,000 employees across various branches and specialized departments. Participants were drawn from four distinct business units: human resources, business intelligence, and two separate client service divisions. This selection ensured a broad spectrum of experiences with different data types, data handling practices, and levels of confidentiality. This aligns with findings from Huaman et al. [68], which emphasize the importance of stratified sampling by role and sector to capture diverse cybersecurity challenges and behaviors. The sample included 13 women and 4 men. On average, they had 6.6 years of working experience, with individual experience ranging from 1 to 23 years. The participants' ages ranged from 25 to 50 with 70.59% aged 25–34, 23.53% aged 35–44 and 5.88% aged 45–54.

Excluding supervisory personnel ensured that responses were uninfluenced by power dynamics, fostering an open discussion. This decision also reflects insights from Huaman et al. [68], who identified variations in cybersecurity awareness and engagement based on job roles, noting that non-technical staff and lower-tier employees often face distinct challenges compared to management. For the demographics within the focus groups please refer to Table 1.

3.3 Ethical Considerations

We followed prevalent principles for ethical psychological research [8] and our institution's recommendations for ethical research based on the Declaration of Helsinki throughout the research process.

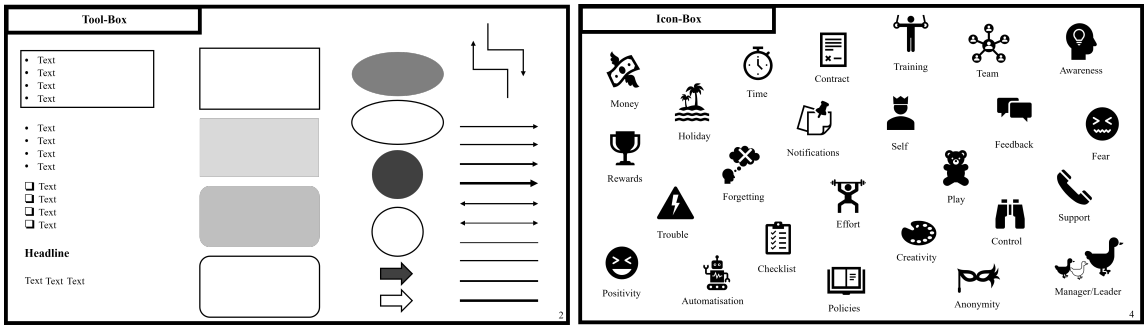


Figure 2: During the brainstorming phase, participants were given a slide featuring a toolbox of elements like arrows and various shapes given on the left side. For the working task, they were free to use any visualization they preferred and could draw inspiration from the toolbox of icons provided on the right side. Icons used are from the Microsoft PowerPoint library.

Table 1: Information on the Sample. For general privacy reasons and to prevent re-traceability of participants, potentially enclosing information on their security behavior that might have negative impacts on their position, we only provide information on the sample within their focus groups.

Group	Gender	Av. age	Av. working experience
Group 1	four females	28 years	5.5 years
Group 2	two females, three males	39 years	9.2 years
Group 3	four females	29 years	7 years
Group 4	three females, one male	32 years	4.3 years
All groups	13 females, four males	32 years	6.6 years

For this type of study no formal IRB process was available in our institution but the responsibility to consider and ensure conformity with ethical and legal requirements rested with the respective researchers and their supervisors. Prior to the interviews, all participants were informed of the purpose of the study, their rights as participants, and the procedures that would be followed. Informed consent was obtained from each participant before the interviews were conducted. Participants were also assured of the confidentiality and anonymity of their responses. After the interviews, the audios were transcribed in an anonymized way and the audio data deleted. The interviews were held in a private and secure setting, and participants had the right to withdraw from the study at any time without experiencing negative consequences. To protect the warranted privacy of our participants, we have intentionally avoided providing overly detailed demographic information, as all participants come from a single company and could potentially be identified. We balance transparency and confidentiality by providing general information in an abstract way to contextualize the study while protecting participant anonymity.

3.4 Data Analysis

We used thematic analysis to analyze the data from the semi-structured interviews and the focus groups [17]. First, all the interviews were read multiple times to gain a thorough understanding of the data. Then, one author coded the material and created an initial set of codes inductively. After the initial coding was complete, another author went through the material and marked any codes that they disagreed with, and added further codes. This process resulted in a merged final set of codes which were then applied to the data. The codes were then analyzed to identify overarching themes and patterns within the data.

4 Results

In the following section, results from the data analysis of the individual interviews, verbal presentation , and the visualizations from the first and second working phases of the focus groups are presented. The findings are organized according to the research questions. We follow the recommendation of Braun and Clarke for synthesizing and contextualizing the data within the results section and provide approximate proportions where applicable to avoid an impression of generalizability in the data [18]. Our codebook is presented in the form of figures within the section dedicated to the respective research question. The text includes exemplary quotes at various points to enhance understanding. Definitions of each (sub)theme are provided in Appendix A.2.

4.1 Attitudes towards Cybersecurity (RQ1)

4.1.1 Affective Component.

Participants expressed varying affective attitudes toward cybersecurity. While almost all participants reported generally *negative feelings*, only half of the sample described *positive emotions* both of which were directly verbalized and labeled. When discussing positive emotions, participants generally expressed a sense of satisfaction or security. For example, one participant noted:

> *"I think it actually gives me a good feeling, especially with the password change (P17)".*

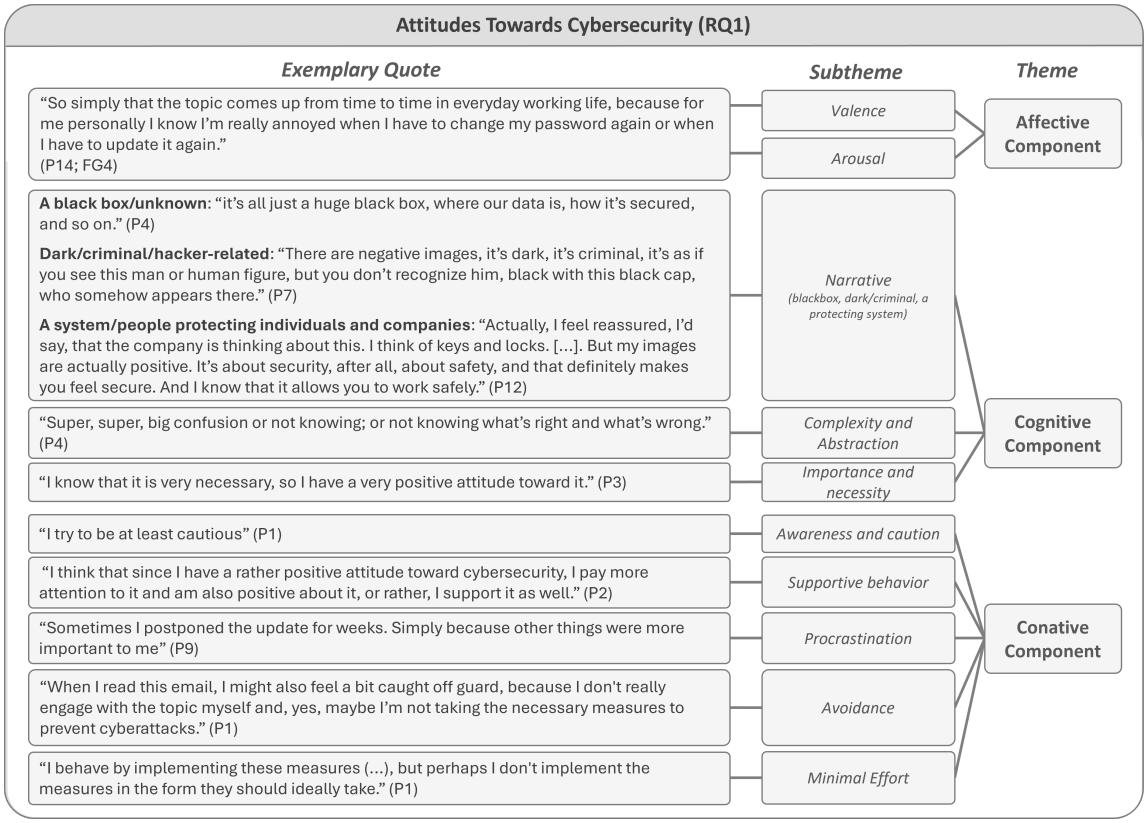


Figure 3: Depiction of the codebook for RQ1

Many participants, particularly those with negative affect, did not elaborate beyond the basic nature of their emotions. However, those who reflected on specific negative emotions primarily mentioned feelings of annoyance, uncertainty, fear, or fatigue with most of them naming the emotion themselves. Other negative emotions that were mentioned once or twice included feelings of stress, shame, guilt, frustration, and boredom. For instance, some participants described feeling ashamed, particularly due to their lack of knowledge or awareness of their inadequate cybersecurity behavior. Importantly, while many participants did not differentiate their positive/ negative emotions, they identified in almost all cases the focus of their emotions. For the focus of their negative emotions, some participants identified specific cybersecurity processes; others referred to cybersecurity itself. A few directed their feelings toward their colleagues' or management's behaviors (see RQ2 for influencing factors) or feelings resulting from their representation of cybersecurity (see cognitive component).

While prior research often does not differentiate the focus of the emotions or between emotion-labels [98], we observed a mix between labeled emotions (e.g., 'fear') and general feelings (e.g., 'negative feelings'). These findings expand upon previous work by demonstrating that emotions related to specific aspects of cybersecurity (e.g., positive emotions about simulated phishing mails) can differ significantly from emotions about the overall concept (e.g., despite positive emotions associated with phishing mails, a negative affective component towards the general concept of cybersecurity). In some cases, these emotions may even contradict one another, as also noted in the research by von Preuschen et al. [97].

Participants also varied in the intensity they perceived the emotions. While some participants expressed strong negative feelings about cybersecurity, others indicated a sense of uncertainty regarding the subject. While not specifically described, participants' emotions varied regarding the level of *arousal*. For instance, word choice (e.g., "a bit annoyed" or "very annoyed") can indicate the level of arousal.

4.1.2 Cognitive Component.

For the cognitive component of attitudes, similar to the affective component, participants were more differentiated towards their negative perceptions. Participants varied in how they articulated

their understanding of cybersecurity, with almost one-quarter describing it *as a "black box", something distant, or unknown* to them. A little over one-third also depicted cybersecurity with *dark, criminal connotations, frequently invoking the image of a black-hooded hacker.* Prior research highlighted that encryption, as part of cybersecurity, is often represented as some kind of black-box [104] and cybersecurity in general represented by noir/dark elements [25, 87]. Roughly one-third viewed *cybersecurity as a system (encompassing the technical system and security professionals), emphasizing its role in safeguarding them from potential threats.* In particular, some framed cybersecurity as the security professionals actions for ensuring the organization's security. In comparison to earlier studies examining the representation of (areas of) cybersecurity [44, 60, 104], the narratives in our study were quite abstract, leaning more towards associations and perspectives rather than concrete models. Participants often highlighted the *complexity* of cybersecurity, describing it as abstract, ungraspable, and difficult to engage with. As one participant portrayed:

> *"For me it's not comparable to physical attacks, [...] of course it's a danger for me and it could theoretically have negative consequences. But it's not the same as, I don't know, terrorist attacks or something else (...) so this physical violence. So, it's not threatening to me in that way. (P1)".*

Despite these negative perceptions, there was a shared recognition of the importance of cybersecurity. The vast majority of participants acknowledged that they viewed cybersecurity as *important*, essential or necessary, though the perceived priority of cybersecurity within their company varied among them. A similar finding was made by Renaud et al. [80], who found that while many participants viewed cybersecurity as complex or fear-provoking, most agreed on the importance of the topic.

4.1.3 Conative Component.

In line with prior work on the conative component outlined in section 2.1, participants either reflected on previous actions or made statements about future intentions. While most participants reflected on their own actions and intentions, some interviewees described cybersecurity actions from an outer perspective. Further, the statements varied in specificity, ranging from descriptions of specific cybersecurity behaviors, such as performing updates, to a general stance encompassing all cybersecurity-related actions. Some individuals expressed a general stance while also providing examples, as illustrated in the following quote:

> *"Everything related to it [(cybersecurity), ...] is simply pushed aside until [...] it can no longer be postponed. For example, updates — I often put them off for as long as possible until they eventually happen automatically, like earlier (P1)".*

This quote further illustrates *procrastination* behavior, which was described by almost one-quarter of participants as the intentional delay of security-related tasks despite the awareness that postponing might result in negative consequences. Sometimes aligning with this theme, the behavioral tendency most often included *minimal efforts* toward cybersecurity, named by more than half of participants. However, this concerned either the intensity of invested energy or the scope of the required efforts. A little over one-sixth of participants stated that they had *avoided* the topic of security altogether.

Regarding favorable behavioral tendencies, a little over one-third of participants expressed a *supportive stance* by directly stating their positive attitude or describing how they adhered to management and expert recommendations when introduced. More than half of the participants reported general *awareness or caution* regarding cybersecurity. However, this view was often not accompanied by specific strategies for behavior and, thus, sometimes encompassed unintentional risky behaviors. For instance, one participant described acting subconsciously secure:

> *"But one should be careful that the data doesn't end up in the wrong hands. However, I think I just do it subconsciously. For me, it's completely normal to pay attention to that. (P16)".*

Overall, participants most frequently discussed behaviors related to locking their screens, managing passwords, identifying phishing emails, and, most notably, performing updates.

4.1.4 Dynamics between components.

Regarding the interaction of the *affective* and *cognitive* component, we observed that participants who perceived cybersecurity as a black box, criminal, or overly complex often reported negative emotions. In contrast, participants who viewed cybersecurity as a system that protects them, tended to feel secure or protected, although this did not necessarily evoke general positive emotions. Notably, more than half of the participants expressed negative emotions while simultaneously acknowledging the importance of cybersecurity.

Concerning dependencies between the *affective* and *conative* components, participants who reported negative emotions such as fear, annoyance, or frustration often described corresponding negative behavioral outcomes, including minimal effort, procrastination, or avoidance tended to exhibit behaviors characterized by awareness or caution (though not necessarily supportive actions; see "conative component") or reliance on minimal effort strategies.

Simultaneously, for *cognitive* and *conative* dependencies, participants who viewed cybersecurity as dark, criminal or a blackbox tended to show unfavorable behavioral tendencies such as procrastination or minimal effort. In contrast, those who viewed cybersecurity as a protective system often demonstrated caution and awareness, while participants who regarded it as important were more likely to display supportive behaviors.

Instances, in which positive *affective*, *cognitive*, and *conative* components are aligned, suggested that participants who feel positive about cybersecurity are more likely to understand its importance and engage proactively. Still, many participants themselves reflected that they had ambivalent attitudes. Almost two-thirds indicated a conflict between perceiving security as important, while having negative feelings about the topic — particularly a general negative feeling concerning cybersecurity, fear or annoyance. Notably, negative feelings often arose from a perceived lack of knowledge, which discouraged individuals from learning more about security — often due to fear of making mistakes. This, in turn, reinforced and deepened their negative emotions, creating a vicious cycle. One participant captured a part of this dynamic with the following quote:

> *"I mean, because it has this somewhat negative influence, the positive aspect, of course, also gets overshadowed... there's always this negative undertone. And, well, you can't really call it fear, but there's definitely a certain sense of uncertainty, maybe because one isn't very familiar with the topic (P5)".*

In line with these results, prior research also indicates that in cases of unfamiliarity with an object, people rely more on the affective rather than the cognitive component of their attitude [93].

Summary RQ1.
Participants displayed a range of affective, cognitive, and conative attitudes toward cybersecurity. They expressed a mix of emotions, from annoyance and fear to security. Cognitively, many viewed cybersecurity as complex and distant, though its importance was recognized. Behaviorally, responses varied from proactive engagement to procrastination and avoidance, often occurring simultaneously. Generally, many participants showed ambivalent attitudes towards cybersecurity. For instance, some participants perceived cybersecurity as very important while having a negative feeling and procrastinating:

> *"So on the one hand I think it makes sense, but on the other hand it's a bit annoying, because after changing my password, my laptop always stops working properly and somehow there are always problems (P15)".*

For an overview of the themes and subthemes, along with exemplary quotes, please refer to Figure 3.

4.2 Factors influencing Cybersecurity Attitudes (RQ2)

4.2.1 *(Social) Experience.*

One of the most prominent factors shaping cybersecurity attitudes was personal experience. Participants described either direct experiences (events they had personally faced) or indirect ones (stories or information about others' incidents). These experiences spanned different time frames, including past experiences (resolved events), ongoing experiences (present encounters), and anticipated experiences (expected future events).

Past Experiences. For past *direct* experiences, participants mostly mentioned their experience with on-boarding processes. Some noted that they had not pursued further cybersecurity learning since then, others described participating in various educational programs. Only a few participants reported experiencing a cybersecurity attack or incident in their organization. Previous research indicates that experiencing security issues at work can increase awareness, thereby influencing attitudes and future security behavior [15].

While only a little over one-sixth of participants experienced incidents, more than one-third described *indirect* experiences made by colleagues, family members, or other companies to have impacted their attitudes. This is in line with previous research highlighting that negative security experiences shared by peers influenced their behavior changes [46, 76]. Additionally, family members and friends were primary sources of physical-security advice, with perceived "tech-savviness" rather than formal education or job roles determining expert status [76].

Ongoing Experiences. Almost half of the participants mentioned that their personal, *direct* experiences with cybersecurity in their private lives strongly influenced their attitudes. In the organizational context, however, cybersecurity was seen as a *barrier to getting their primary work tasks* done by more than half of the participants. They perceived security requirements, like frequent password changes, unreasonable, criticize the usability of security software, and felt that security measures tend to appear at the most inconvenient times. This extends previous research that has identified time-consuming requirements and the general inconvenience of security measures as contributors to security fatigue [24].

In contrast, *indirect* experiences stemmed from how cybersecurity is portrayed in the media, organizational culture, or management's priorities. Related work on the portrayal of cybersecurity in the media demonstrated that user beliefs are shaped by the media depictions and, in case of incorrect portrayals, can foster cybersecurity misconceptions [44, 74]. Even people with technical backgrounds could better distinguish between reality and media depictions but were not completely immune to their influence [10]. Still, media is often used a source for security advise [75]. Half of the participants reflected how social evaluations of themselves or perceptions of their colleague's behavior – sometimes in comparison to themselves from social interactions – influenced their attitudes.

Future Experiences. For the *direct* future perspective, almost one-third of participants expressed fear of making mistakes and the potential consequences. Concerns ranged from social consequences, such as being blamed, to more severe outcomes like job loss. Participants also worried about the broader impact on the company. For *indirect* experiences, a few participants mentioned how others' concerns, such as the financial impact of cyberattacks on their organization, influenced their own attitudes.

4.2.2 *Individual Factors.*

Individual factors were also found to influence attitudes toward cybersecurity. Participants expressed varying perceptions of vulnerability, with some feeling a lack of knowledge or viewing cybersecurity as distant, while others noted discrepancies between their knowledge and behavior. Contextual variables also played a key role, such as the sensitivity of data and the perceived lack of support. Two social factors stood out: the level of perceived social support (e.g. *"there's no one I can turn to (...) or where I would know where to go now. (P1)"*) and feelings of being excluded from the organization's security strategy (e.g. *"But it [the communication on security] often comes too late (P8)"*). Interestingly, despite all participants experiencing the same cybersecurity awareness measures as they were part of the same organization, not all participants felt adequately informed about cybersecurity. Yet, others reported feeling overwhelmed by the volume of cybersecurity-related emails they received. Additionally, participants had varied perceptions of what constitutes a cybersecurity incident and differed in their ability to recall recent incidents.

Summary RQ2.
Cybersecurity attitudes are primarily driven by direct and indirect experiences varying in their temporal distance (past, ongoing, future), along with individual factors including perceptions of context factors. Both areas are highly influenced by social factors such as

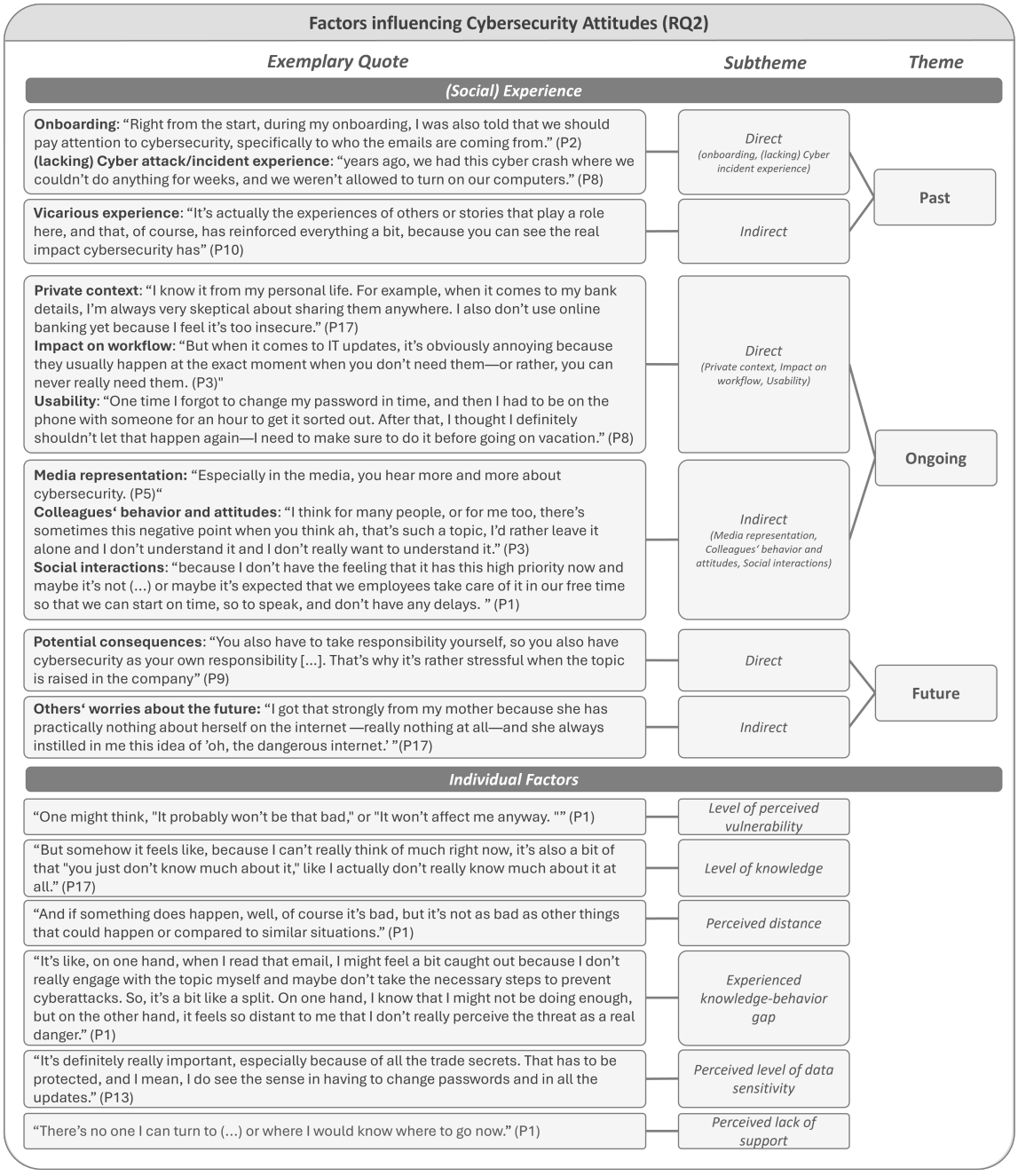


Figure 4: Depiction of the codebook for RQ2

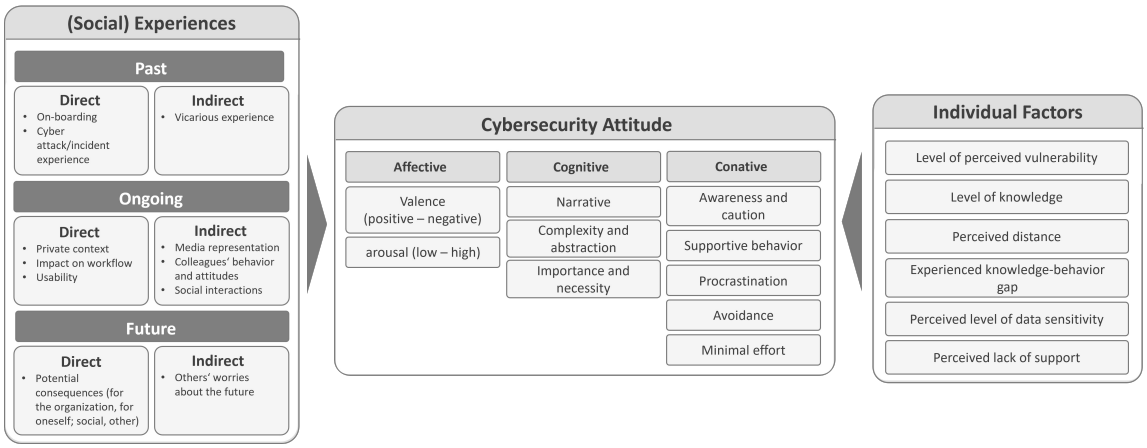


Figure 5: Visualization of the results related to RQ1 and RQ2

social interactions or perceived lack of support that are embedded within *(social) experiences* and *individual factors*. For a visual summary of the findings for RQ1 and RQ2, please refer to Figure 5. For an overview of the themes and subthemes of RQ2, along with exemplary quotes, please refer to Figure 4.

4.3 Employees' Needs for Positive Cybersecurity Attitudes (and Positive Cybersecurity Behavior; RQ3)

4.3.1 Social and Cultural Framework.

Management Security Actions. Nearly all participants emphasized the need for clear management handling in prioritizing cybersecurity. They suggested that management should actively communicate cybersecurity as a top priority and model the desired security culture accordingly. Two participants explicitly emphasized that management should lead by example and serve as role models in cybersecurity practices. Additionally, participants called for well-defined roles and responsibilities, such as appointing specific contact persons for cybersecurity issues.

Social Acceptance. A little over one-third of participants expressed the feeling that they are not permitted to take time from their regular work for cybersecurity tasks. They were concerned that colleagues might view them as lazy or be annoyed by their focus on cybersecurity rather than primary work tasks. Others worried about losing valuable work time, as one participant stated:

> *"Also, that [management] allocates time for me to engage with the topic and takes it seriously [...] and that I don't have to postpone it to after my work hours, to the evening, but that I can actively dedicate time to it during the workday, and that it should be prioritized accordingly. Perhaps this would alleviate some of the fear (P1)".*

As a consequence, during all focus groups participants indicated a preference for mandatory cybersecurity training for everyone.

User Inclusion in Cybersecurity Processes. Three focus groups and some individuals expressed a desire to be actively involved in the security process, such as through providing feedback. However, simultaneously all focus groups indicated a need for more external support or dedicated contact persons. As one participant suggested:

> *"The contact persons must be defined, i.e., there must be a manager or leader who is practically in charge. However, they must also always coordinate with other teams. There should always be a constant exchange between the units (P10, FG2)".*

Team Security Vision. Slightly less than half of the participants noted that changing attitudes toward cybersecurity depends heavily on collective attitudes. They emphasized the need for opportunities to learn about security together and to frame cybersecurity as a shared goal. Two participants in particular described they needed their colleagues to show a positive attitude or desirable security behaviors in order to have a positive attitude themselves. In particular, many desired everyday conversations about cybersecurity in particular exchanging their perspective on cybersecurity with their colleagues. For instance one participant noted:

> *"Sometimes it helps to exchange views somehow or to realise that hey, [...] this is annoying us all, why don't we go for a coffee in the meantime? (P6)".*

Yet, some described feeling unsure if they could annoy their colleagues with a topic they think others perceive negatively. Some suggested (social) incentives for positive cybersecurity behavior as described by one participant:

> *"Then an update comes in and that's exactly the time when we can get together here on the phone or [...] meet and have a coffee together and just take a short break [...] it would [...] of course be cool [...] so let's hope that more updates come in today. Because at the moment it's more like 'oh man, I have to finish this [work task] now and it's totally inconvenient and now*

> *I have to interrupt the task to do it'. Maybe you could set this as a kind of networking task in the company, for the time in the update, so that you link something cool to it, so that you know that you don't have any time pressure right now, which is additionally intensified by some update, [...] but think 'oh cool now is the time now I can do this and that, which is also allowed and encouraged by the company'. (P3)".*

Security Decision Autonomy. Despite the expressed need for collectivity, some participants described that they needed more autonomy, for instance, being able to decide on their software update or password renewal times themselves.

Security as a Process. All focus groups suggested to foster positive cybersecurity attitudes through a process with several steps. Despite naming different process steps with a different focus, all results included at least four steps. The steps outlined are categorized within the themes and subthemes of RQ3. This section provides a high-level overview of the processes involved, while more detailed descriptions will be presented in the corresponding sections.

All groups stress the importance of feedback and looping the process if needed. While some refer to a clear linear structure, others draw a feedback process that allows going back and forth where needed. Two groups proposed beginning by raising awareness about security. Another group suggested the establishment of the necessary infrastructure and reflecting on negative emotions related to the topic, while the final group emphasized the management's clear responsibility to communicate the importance of security to the teams. Additionally, two groups highlighted the significance of analyzing the current state to develop tailored approaches. These could be employee-centered (conducting a survey to gauge employee sentiments about cybersecurity), infrastructure-centered (assessing if the technical infrastructure meets the organization's needs), or action-centered (evaluating what has already been implemented). Three groups specifically mentioned the need for a 'training' phase, while one group viewed the technological implementation as equally important as employee actions within a 'conduct' phase. Moreover, three groups recommended a process of habituation, suggesting methods such as notifications, general reminders, and rewards. For a visualization of the workgroup phases, please refer to section Appendix A.3.

Technical Framework and Infrastructure. Participants emphasized that a robust technical framework and infrastructure form the foundation of organizational cybersecurity. Without this essential groundwork, employees feel that their efforts are ineffective. Furthermore, many participants recommended analyzing the security state of the company and the awareness level of their employees together with a custom analysis of the needs of the company. Based on that, a tailored security approach should be designed that encompasses individual human-centred security strategies and technical solutions.

4.3.2 Communication Style.

Security Simplicity and Usability. For the style of communication, almost two-thirds of participants stated they needed short, clear, and easy communication but also usable learning materials and security measures (such as the interface of two-factor authentication). This need is reflected by a multitude of studies as well as theories used in security research such as the technology acceptance model [28, 29, 84].

Positive Security Mindset. Almost half of the participants also desired a positive communication style that encourages compliance through self-affirmation rather than coercion. They preferred a focus on enhancing positive emotions, such as pride, and reducing negative feelings. They pointed out that communication should highlight successes as well as areas for improvement. Additionally, they suggested using incentives like awards or praise to cultivate positive attitudes toward cybersecurity.

Security Tangibility and Branding. One focus group suggested leveraging marketing tools or something graspable like branded sticky notes, plush toys, or pens to enhance cybersecurity awareness.

Transparent Security Actions and Communications. Participants emphasized the need for transparent cybersecurity communications. Almost all participants stressed the importance of communicating transparently. This ranges from updates on the security strategy, management decisions, considerations for future security measures to clear information on the time required for implementing security protocols and participating in training. Additionally, some felt out of the loop during incidents, noting that updates often came too late. However, even with transparent risk communication, the style should avoid inducing excessive fear, as one participant noted:

> *"[The dangers] simply have to be made clear, because I think a lot of damage can be done and of course you shouldn't scare people into not passing on certain information, (...) that they end up preventing themselves from doing so (P17)".*

4.3.3 Education Contents.

Security Knowledge Enhancement and Transfer. Over half of the participants expressed a need for more knowledge and experience in cybersecurity. They specifically highlighted a lack of understanding about the reasons behind cybersecurity (not just their importance, but also clear explanations of why implementing them is essential), consequences (the impact of cyberattacks and the risks of not implementing security measures) and practical action strategies. For instance, one participant suggested: *"At the beginning [we need] some kind of training where employees are explained why the whole thing is important and what the consequences are if [we] don't establish the whole thing (P16, FG4)"*, while another participant desired clarification on *"what is behind it and what effects it could have and how you can naturally protect yourself and accordingly develop a safer feeling for it (P2)".*

Security Scenarios and Stories. Almost half of the participants expressed a desire to learn from real-world examples, such as cyber incidents in similar companies, which they believe would motivate action:

> *"but if you point out that things have gone wrong at other companies or give negative examples. I think then everyone is directly more motivated to do something about it so that it doesn't happen to them (P16)".*

Others suggested fictional examples, yet, presented with real emotions to illustrate the relevance of cybersecurity and engage

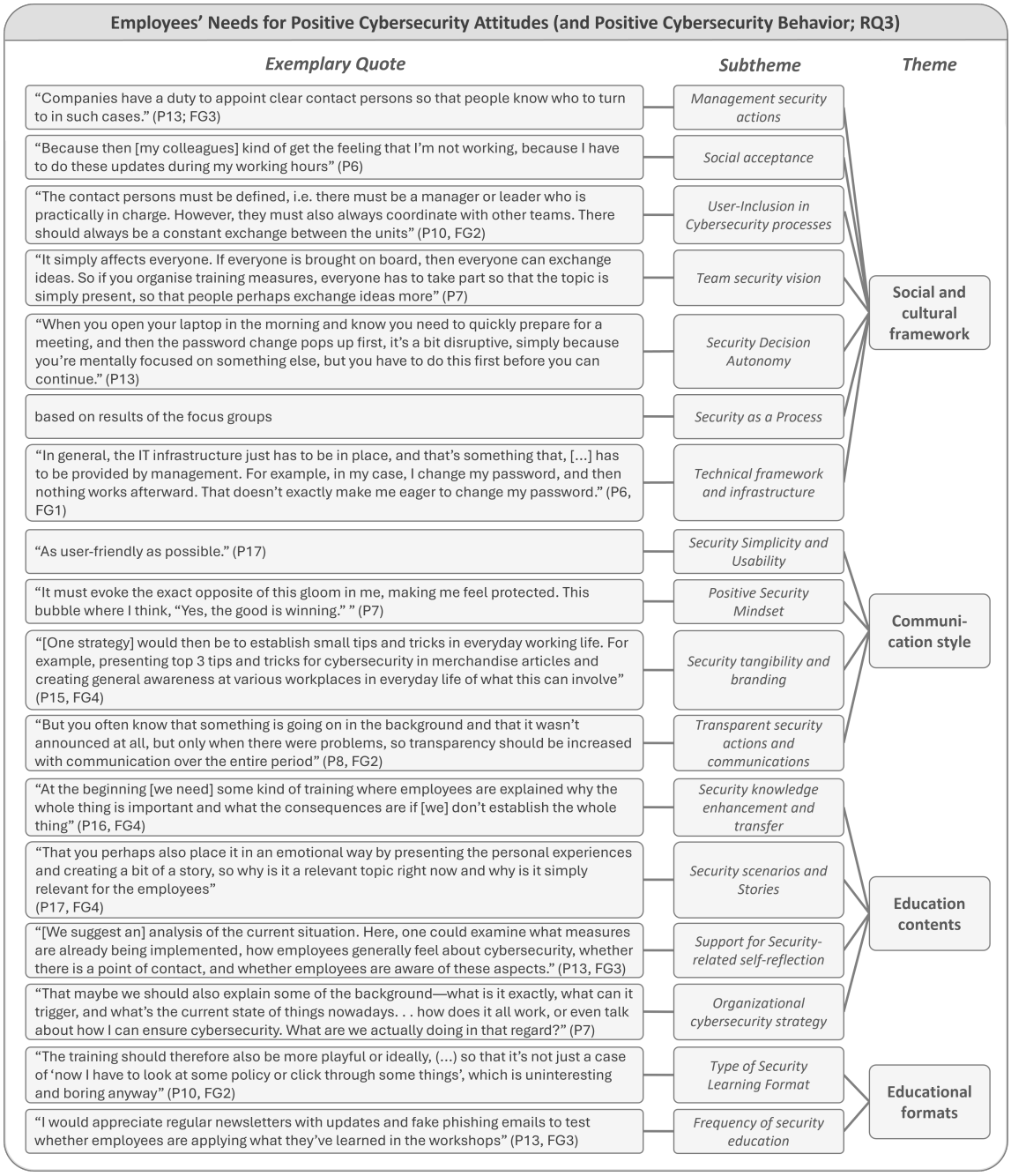


Figure 6: Depiction of the codebook for RQ3

employees on a deeper level. In line with that, previous work demonstrated how anecdotes and informal stories can serve as valuable security education [71, 73].

Support for Security-related Self-reflection. Almost half of the participants expressed the need for support in self-reflecting on their cybersecurity skills, security-related attitudes or ongoing feedback processes in general. This involved, on the one hand, assessing their current abilities and identifying areas for improvement, such as through testing in areas like authentication management or phishing detection. On the other hand, it includes reflecting on their attitudes toward cybersecurity, with a particular emphasis on the emotional aspect. This approach aligns with the concept of using a positive and constructive communication style, emphasizing strengths while transparently addressing areas for improvement (see *communication style*). The need for self-reflection aligns with findings demonstrating the positive effect of reflective writing intervention by Krsek et al., which aims to enhance self-awareness and align knowledge with action [61].

Organizational Cybersecurity Strategy. One-third of participants expressed a need for technical protection measures, such as antivirus software or two-factor authentication. Interestingly, these protections are usually already implemented. Therefore, the real need lies in fostering a sense of technical security, which can be achieved through targeted training and awareness initiatives. Further, as described in the need of user integration, this entails briefing users on current cybersecurity efforts to ensure they feel informed and supported.

4.3.4 Educational Formats.

Type of Security Learning Format. Participants expressed a need for diverse educational formats, including group workshops, online and on-site training, and databases. While a little less than one-quarter of participants specifically requested digital learning resources, almost one third expressed a preference for workplace-based learning, including in-person workshops. Although interviewees acknowledged the importance of policies, they generally viewed policy-focused training negatively. Instead, participants stated they required engaging, easy-to-understand, and fun learning contents. One-third of participants also highlighted the need for gamified and visually appealing training, emphasizing that these should be short, easily integrated into daily work, and offer a sense of reward, such as inducing pride. Additionally, participants who found cybersecurity abstract desired hands-on experiences, such as simulations or phishing campaigns. Some participants viewed simulated phishing campaigns as personal challenges, emphasizing that they appreciated being regularly engaged with cybersecurity in this way. In line with these needs, several previous studies have highlighted the positive impacts of personalized education, however, research specifically in cybersecurity is still limited [42, 85]. Extending prior positive findings of group trainings, many participants specifically expressed the importance of training in realistic group settings[23].

Frequency of Security Education. One-third of participants expressed a need for not just more frequent cybersecurity education but also more consistent training intervals. While few specified exact numbers, those who did suggested 2-4 sessions per year. To reinforce their learning, participants highlighted the importance of regular reminders of previously communicated information. They suggested using diverse formats such as newsletters, simulated phishing campaigns, flyers, or checklists.

Summary RQ3.
Employees identified several needs related to positive cybersecurity attitudes. They emphasized the importance of minding factors within a social and cultural framework, communication style, educational contents, and educational formats. Additionally, participants emphasized the significance of treating attitude change as a process, with varying requirements at different stages, such as more comprehensive educational initiatives at the start, followed by periodic reminders to sustain engagement over time. Notably, participants did not distinguish between needs for promoting positive attitudes and positive security behaviors. For an overview of the themes and subthemes, along with exemplary quotes, please refer to Figure 6.

5 Discussion

Attitudes are a major predictor for behavior and learning success [2, 5, 22] - areas, that are highly relevant to human-centered cybersecurity strategies. Thus, with the use of interviews and focus groups this paper aims to explore cybersecurity attitudes as a complex construct from a holistic perspective minding social influences. While previous studies often relied on quantitative surveys or single-method qualitative approaches, our study combines personal reflections with group discussions to reveal cybersecurity attitudes, the factors influencing them, and the needs for improved cybersecurity attitudes and behaviors. Prior research demonstrated a high relevance of attitudes in the field of cybersecurity [30, 52, 70] – our research underscores these results. We present a summary of the alignment, extensions, and disconnections of the most prominent results with prior literature in Table 2.

To date, there is a lack of research addressing cybersecurity attitudes as a multifaceted construct with most literature focusing on the cognitive or conative component. However, as demonstrated by de Kok et al. [30], our research highlights that attitudes indeed are complex encompassing various parts including affective, cognitive, and conative components. Additionally, we identified a frequent attitudinal ambivalence toward cybersecurity, further illustrating that attitudes are a complex construct shaped by the interplay of these various components.

Furthermore, factors influencing cybersecurity attitudes have largely been examined within specific contexts, such as multi-factor authentication and security notifications [9, 38]. Our research goes beyond specific contexts, suggesting that it is not the triggers themselves, like multi-factor authentication or security notifications, but rather the underlying factors (as identified in RQ2) that shape cybersecurity attitudes. Further, consistent with research on attitudes [37, 77], we find that experiences majorly influence cybersecurity attitudes, alongside individual factors and perceptions of contextual factors.

Additionally, our research delves into employee needs, aiming to foster positive cybersecurity attitudes and promote proactive cybersecurity behaviors. For instance, contrasting with negative emotions found by Arnold et al. [9], many participants in our study suggested implementing multi-factor authentication themselves.

	Alignment with previous work	Disconnects and extensions related to previous work
RQ1	- Confirming that cybersecurity is viewed as important [80] - Validating the relevance of the affective component within cybersecurity attitudes [30, 93, 97] - Confirming primarily negative emotions, but also positive ones particularly feeling secure or protected [36, 97, 98] - Finding similar narratives to prior research [25, 87, 102] - Displaying complex behavioral tendencies (e.g., within "minimal effort" employees might show desirable behavior, but actually practice workarounds) [13, 97]	- Extending literature on mental models (inner representation of cybersecurity; e.g., [44, 60, 104]) by displaying cognitive evaluations and affective associations within narratives - Underscoring the relevance of the focus of emotions (e.g., fear of making mistakes vs. fear of cyber attacks) - Identifying "awareness and caution" as a theme that may be potentially associated with unfavorable behavioral consequences - Uncovering an interplay between the three components of attitudes (with the affective attitude being particularly relevant) - Identifying mixed attitudes and ambivalence
RQ2	- Validating that prior experience can increase awareness and influences future security behaviors [15] - Confirming the influence of peers' negative security experiences on attitudes/behavior changes [76] - Showing time-consuming requirements and the general inconvenience of security measures as contributors [24] - Confirming media as a major influence on attitudes [44, 74, 75]	- Uncovering an awareness of discrepancies between knowledge and behavior as an influence on security attitudes - Providing new insights into how employees within the same organization can have differing perceptions of cybersecurity measures and incidents - Extending knowledge on how social evaluations, self-perceptions in a social context, and comparisons with/evaluations of colleagues' behavior influence cybersecurity attitudes [40, 46, 75, 97] - Uncovering how others' concerns, such as financial impact of cyberattacks, influence individual attitudes - Enhancing the understanding of social interactions regarding security, particularly the perceived lack of support, management actions, and team discussions - Displaying that some feel like they are not allowed to do security tasks during their work time; others might think they avoid their work
RQ3	- Confirming security simplicity and usability as relevant for positive attitudes and behaviors [28, 29, 84] - Showing security scenarios and stories as relevant for positive attitudes and behaviors [71, 73] - Validating knowledge as relevant for positive attitudes and behaviors [70]	- Uncovering needs derived from individual perspectives and collective discussions - Displaying unsuitability/undesirability of gamification/"fun" for all areas of cybersecurity - Introducing the need to view security as a process - Uncovering the need for a positive security mindset that helps to reflect what is already going well and to implement positive communications - Providing new insights into the need to adapt the emotional tone according to the respective phase - Extending needs for personalization of education in the context of cybersecurity [42, 85] - Extending prior positive findings of social factors in education by displaying collective needs [23]

Table 2: Overview of the most relevant alignments, extensions and disconnects related to previous work

Yet, for positive attitudes towards cybersecurity and the implementation of favorable behavior, a range of needs requires to be addressed. Based on our findings, several recommendations can be derived, in particular from RQ3 (e.g. *Positive Security Mindset* and *Transparency* - implement communication strategies that are self-affirming yet provide transparent feedback on areas for improvement). Here, we present three key recommendations informed by our and related prior research findings.

5.1 Recommendations for Human-centered Security Strategies

Go beyond Fear, Fun, or None. We observed that participants expressed diverse needs in communication styles throughout different phases of the cybersecurity strategy. These ranged from fear-inducing communication (such as transparent communication about risks), fun elements (such as gamification), and neutral communication (such as reminders). Participants emphasized that excessive fear can lead to avoidance, aligning with the observations made by von Preuschen et al [97].

In line with that, studies demonstrate that high levels of fear can result in psychological distancing from cybersecurity in general [21, 97]. While findings on the efficacy of fear appeals are mixed overall, research suggests not using them on their own but always combining them with information on how to cope with the threat [33]. Also, inducing fear in employees warrants ethical considerations for which Dupuis et al. [34] have developed an initial set of guidelines. Research on the use of personal stories to promote security and privacy behavior shows that they can serve as educational elements [71, 73] and that relatable stories can evoke negative emotions, yet, ultimately increasing attention [49]. Thus, while fear might be beneficial to draw attention to the topic, there is a risk that employees distance themselves from the topic if emotions are maintained.

As a result, we strongly recommend addressing and resolving negative emotions that are already or were intentionally connected with cybersecurity. This aligns with previous research, which shows that storytelling is highly effective in influencing behavior and attitude changes, especially when it involves emotional shifts. Emotional shifts engage individuals, stimulate curiosity, and encourage them to share their experiences with others [67]. Further, resolving fear can result in courage, empathy and increased prosocial behavior [64]. In contrast, despite positive effects of appeals invoking positive emotions [47], positive emotions towards cybersecurity can also result in unfavorable behavior [21, 97]. Our results provide a new perspective on this issue by highlighting a potential attitudinal dissonance between communication strategies and employees' attitudes. For example, humorous communication about cybersecurity may clash with employees' perceptions of cybersecurity as a serious matter not to be taken lightly. Therefore, we recommend first empathizing with the employees, introducing emotions that are suitable for the needs throughout the respective phase. For instance, as many participants expressed fear towards cybersecurity, communications in a early stage could address their fears (e.g., by transparently communicating risks) and, thus, should align with their emotional experiences. Finally, negative emotions should be resolved and shifted towards positive ones. These stages, aligning with positive attitudes, then allow for the usage of fun elements. This underscores the importance of offering diverse learning formats and communication styles tailored to employees' needs. First approaches towards personalized cybersecurity communication or training include cybersecurity learning in general [86], personalized security warnings [106], and personalized phishing training [85].

Foster Self-reflection. We found that (social) experience and individual factors including perceptions of context factors influence cybersecurity attitudes. (Social) Experiences, yet, can be an influencing factor for individual factors itself. We observed that even minor negative experiences - sometimes not directly related to cybersecurity - can negatively impact general attitudes towards cybersecurity. For instance, employees reported negative experiences of updates influenced their overall cybersecurity attitude. This aligns with Vaniea at al. [94], who found that users often do not distinguish between feature updates and security updates. Consequently, any negative experience, including unexpected user interface changes, can be mistakenly attributed to cybersecurity, leading to negative attitudes. Furthermore, we observed negative experiences, such as incident experiences, that resulted in positive attitudes and behavioral tendencies. Yet, these experiences can over time also result in overconfidence in handling future attacks (e.g., through hindsight bias) [81]. Additionally, the accessibility and content of these incident-related memories may deteriorate over time, potentially distorting how the event is recalled [103]. To mitigate these risks, it is crucial to regularly test or actively reflect on one's experiences and attitudes [92]. This approach not only reduces the likelihood of overconfidence but also aids in tailoring educational strategies to better meet employees' needs.

Based on the observed needs, we recommend incorporating real-world experiences or simulations into cybersecurity training. However, it is crucial to introduce these strategies carefully and thoughtfully [96]. Importantly, employees are generally willing to contribute to improving the organization's cybersecurity, provided their needs are considered. Research on emotions shows that putting in significant effort can lead to feelings of pride, which in turn fosters higher engagement [102]. Therefore, communication strategies should emphasize positivity, acknowledging that employees are already doing a good job, and then suggest areas for improvement based on individual needs and performance. Beyond addressing emotions, participants generally desired personal stories to help them emphasize with the given example or persona and close the gap of feeling distant from cybersecurity. This is particularly important given that individuals often perceive themselves as less likely than their peers to be the target of an attack, a phenomenon known as optimism bias [101]. Overall, we recommend self-reflection as a tool to help individuals better understand their attitudes toward cybersecurity and uncover the underlying factors shaping those views. This process can ultimately promote more positive attitudes toward cybersecurity.

Implement a Social Perspective on Cybersecurity Attitudes. Despite individual differences in needs and attitudes, we observed that social dynamics highly influence cybersecurity attitudes. Notably, employees' attitudes were shaped indirectly by experiences from others (e.g., incident experience from other employees or companies) or social interactions including potentially resulting evaluations. This aligns with prior research highlighting the influence of social triggers on cybersecurity behavior, both positive and negative [26, 27, 66]. Extending beyond this research, we examined the role of social factors within the organizational context where they appear at multiple levels—from organizational culture and team dynamics to interpersonal interactions. A key finding was that employees feared being perceived negatively by their colleagues for engaging in security-related tasks during work hours, which they felt might detract from their primary responsibilities. Our research also uncovered several social needs, including the desire for social incentives, team envisioning, management actions and colleagues' behavior. However, participants reported a general lack of communication about security, beyond occasional venting. This reflects the findings of Gerber and Marky [46], who identified barriers to security discussions, such as avoiding negative feedback or lacking the right opportunities. Based on these insights, we recommend considering the social nature of attitudes in each strategy decision, extending beyond cultural approaches to include team dynamics and social interactions. For example, this

can be achieved by cultivating psychological safety within teams and encouraging conversations about security.

5.2 Limitations and Future Research

While we identified several factors influencing cybersecurity attitudes, our interview guide did not thoroughly explore the interdependencies among the components of these attitudes and behaviors. Therefore, future research could delve deeper into the dynamics of influencing factors, attitude components, behavior, and their interdependencies. Additionally, further studies could explore the consequences that arise from these dynamics. Qualitative studies, especially focus groups, offer rich insights into social dynamics but often lack broad generalizability. In particular, while our data was collected from employees of various departments, yet within a single company, the results may reflect organizational dynamics, potentially missing out on contextual factors. This limits the generalizability of the findings to other organizational settings. Future research could investigate attitudinal dynamics quantitatively minding multiple organizational backgrounds and contextual factors. Due to the small sample size, we may have overlooked differences related to departmental affiliation. Future research, using larger sample sizes, could explore industry or departmental differences in greater depth.

Moreover, we first, observed that cybersecurity attitudes are significantly influenced by social factors, such as social evaluations and interactions. Second, our findings reveal various components within attitudes, including instances of attitudinal ambivalence (e.g., while employees may recognize the importance of cybersecurity behaviors and even engage in them, they might procrastinate, ultimately performing the desired actions too late). Both of these nuanced aspects are often overlooked in current measurement tools. Therefore, future research should consider developing a measurement tool that incorporates both a social and holistic perspective on organizational cybersecurity attitudes.

5.3 Conclusion

Employees' attitudes towards cybersecurity are increasingly recognized as a relevant driver for secure behaviors and thus organizational security overall. However, security-related attitudes, their influencing factors and impacts, are not yet well understood within the complex organizational setting that includes not only individual, but also social aspects. To shed light on employees' security-related attitudes, how these shape behaviors, and employees need for attitude change, we conducted a combination of in-depth individual interviews and focus groups with employees from the same organization. Through analyzing the emerging affective, cognitive, and behavioral components of attitudes we identified a range of attitudes. Exemplary, these encompass feelings of annoyance and fear (affective component), appreciation for cybersecurity measures (cognitive component) or varying behavioral tendencies ranging from a supportive stance to avoidance (conative component). Personal direct experiences (e.g., in onboarding processes) and indirect experiences (e.g., hearing anecdotes from peers) as well as individual perceptions (e.g., perceived social support) were identified as key influences on attitudes. The social component was prominent for all of these aspects. In line with that, for developing positive attitudes, employees referred to the company's social and cultural framework, communication styles, educational contents, and formats. Thereby, our study highlights the relevance of taking a social perspective on cybersecurity attitudes and moving beyond purely individual-focused cybersecurity measures and assessments.

6 Data Availability Statement

Due to the sensitivity of interviews transcripts with regard to the potential identification of participants, particularly due to the small sample size and the single company context, the interview data is not openly available but can be directly requested from the authors. Sample information, the interview guide, codebook, and exemplarily quotes are provided in the article and Appendix for transparency.

References

[1] Damianus Abun, Theogenia Magallanes, Sylvia Lalaine Foronda, and Mary Joy Incarnacion. 2019. Investigation of Cognitive and affective Attitude of Teachers toward Research and their behavioral Intention to conduct Research in the Future. *Journal of Humanities and Education Development* 1, 5 (2019), 219–232. https://doi.org/10.22161/jhed.1.5.2

[2] Lewis R Aiken Jr. 1976. Update on attitudes and other affective variables in learning mathematics. *Review of educational research* 46, 2 (1976), 293–311.

[3] Icek Ajzen. 1989. Attitude structure and behavior. In *Attitude structure and function*. Lawrence Erlbaum Associates, Inc, Hillsdale, NJ, US, 241–274.

[4] Icek Ajzen. 1991. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (1991), 179–211.

[5] Icek Ajzen. 1993. Attitude Theory and the Attitude-Behavior Relation. In *New Directions in Attitude Measurement*, D. Krebs and P. Schmidt (Eds.). Walter de Gruyter, Berlin, Germany, 41–57.

[6] Icek Ajzen, Martin Fishbein, Sophie Lohmann, and Dolores Albarracín. 2005. The Influence of Attitudes on Behavior. In *The Handbook of Attitudes*, Dolores Albarracín, Blair T. Johnson, and Mark P. Zanna (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, USA, 173–221.

[7] Gordon Willard Allport. 1935. Attitudes. In *Handbook of Social Psychology*. Clark University Press, Worcester, MA.

[8] APA. 2017. *Ethical principles of psychologists and code of conduct*. American Psychlogical Association. https://www.apa.org/ethics/code

[9] Davis Arnold, Benjamin Blackmon, Brendan Gibson, Anthony G Moncivais, Garrett B Powell, Megan Skeen, Michael Kelland Thorson, and Nathan B Wade. 2022. The emotional impact of multi-factor authentication for university students. In *ACM CHI Conference on Human Factors in Computing Systems - Extended Abstracts*. ACM, New York, NY, USA, 1–4.

[10] Khadija Baig, Elisa Kazan, Kalpana Hundlani, Sana Maqsood, and Sonia Chiasson. 2021. Replication: Effects of Media on the Mental Models of Technical Users. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Berkeley, CA, 119–138. https://www.usenix.org/conference/soups2021/presentation/baig.

[11] Ryan J Baxter, D Kip Holderness Jr, and David A Wood. 2016. Applying basic gamification techniques to IT compliance training: Evidence from the lab and field. *Journal of information systems* 30, 3 (2016), 119–133.

[12] Nils Begou, Jérémy Vinoy, Andrzej Duda, and Maciej Korczyński. 2023. Exploring the dark side of ai: Advanced phishing attack design and deployment using chatgpt. In *2023 IEEE Conference on Communications and Network Security (CNS)*. IEEE, New York, NY, USA, 1–6.

[13] Odette Beris, Adam Beautement, and M. Angela Sasse. 2015. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (Twente, Netherlands) *(NSPW '15)*. Association for Computing Machinery, New York, NY, USA, 73–84. https://doi.org/10.1145/2841113.2841119

[14] Igor Bilogrevic and Martin Ortlieb. 2016. " If You Put All The Pieces Together..." Attitudes Towards Data Combination and Sharing Across Services and Companies. In *Proceedings of the 2016 ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 5215–5227.

[15] John M Blythe and Lynne Coventry. 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior* 87 (2018), 87–97.

[16] Scott R Boss, Dennis F Galletta, Paul Benjamin Lowry, Gregory D Moody, and Peter Polak. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly* 39, 4 (2015), 837–864.

[17] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[18] Virginia Braun and Victoria Clarke. 2013. *Successful Qualitative Research: A Practical Guide for Beginners*. SAGE Publications, London, UK.
[19] Steven J Breckler. 1984. Empirical validation of affect, behavior, and cognition as distinct components of attitude. *Journal of personality and social psychology* 47, 6 (1984), 1191.
[20] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.
[21] AJ Burns, Tom L Roberts, Clay Posey, and Paul Benjamin Lowry. 2019. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research* 30, 4 (2019), 1228–1247.
[22] Lang Chen, Se Ri Bae, Christian Battista, Shaozheng Qin, Tianwen Chen, Tanya M Evans, and Vinod Menon. 2018. Positive attitude toward math supports early academic success: Behavioral evidence and neurocognitive mechanisms. *Psychological science* 29, 3 (2018), 390–402.
[23] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 2024. The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–21. https://doi.org/10.1145/3613904.3641943
[24] W Alec Cram, Jeffrey G Proudfoot, and John D'Arcy. 2021. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal* 31, 4 (2021), 521–549.
[25] Joseph Da Silva and Rikke Bjerg Jensen. 2022. "Cyber security is a dark art": The CISO as Soothsayer. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 365 (Nov. 2022), 31 pages. https://doi.org/10.1145/3555090
[26] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 97–115. https://www.usenix.org/conference/soups2019/presentation/das
[27] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) *(CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 1416–1426. https://doi.org/10.1145/2675133.2675225
[28] Fred D Davis. 1989. Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology. *MIS quarterly* 13, 3 (1989), 319–340.
[29] Fred D Davis, RP Bagozzi, and PR Warshaw. 1989. Technology acceptance model. *J Manag Sci* 35, 8 (1989), 982–1003.
[30] Lisa C de Kok, Deborah Oosting, and Marcel Spruit. 2020. The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security* 46, 3 (2020), 251–266.
[31] Tamara Dinev, Jahyun Goo, Qing Hu, and Kichan Nam. 2009. User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal* 19, 4 (2009), 391–412.
[32] Tamara Dinev and Qing Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8, 7 (2007), 23.
[33] Marc Dupuis, Anna Jennings, and Karen Renaud. 2021. Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene. In *Proceedings of the 22nd Annual Conference on Information Technology Education* (SnowBird, UT, USA) *(SIGITE '21)*. Association for Computing Machinery, New York, NY, USA, 35–40. https://doi.org/10.1145/3450329.3476862
[34] Marc Dupuis and Karen Renaud. 2021. Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology* 23, 3 (2021), 265–284.
[35] Marc Dupuis, Karen Renaud, and Anna Jennings. 2022. Fear might motivate secure password choices in the short term, but at what cost?. In *Hawaii International Conference on System Sciences*. IEEE, Hawaii, USA, 1–10. https://strathprints.strath.ac.uk/77671/
[36] M. Dupuis, R. Searle, and K.V. Renaud. 2025. Finding Grace in Responses to Adverse Cybersecurity Incidents. *Journal of Intellectual Capital* 26, 1 (2025), 45–70. https://doi.org/10.1108/JIC-04-2024-0128
[37] Leandre R Fabrigar, Tara K MacDonald, and Duane T Wegener. 2005. The structure of attitudes. *The handbook of attitudes* 80 (2005), 79–124.
[38] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. 2015. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior* 51 (2015), 504–519.
[39] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2022. Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13). arXiv:2204.03114 [cs.CR] https://arxiv.org/abs/2204.03114
[40] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2024. A Framework for Reasoning about Social Influences on Security and Privacy Adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 16, 13 pages. https://doi.org/10.1145/3613905.3651012
[41] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, 61–77. https://www.usenix.org/conference/soups2019/presentation/faklaris
[42] Rida Indah Fariani, Kasiyah Junus, and Harry Budi Santoso. 2023. A systematic literature review on personalised learning in the higher education context. *Technology, Knowledge and Learning* 28, 2 (2023), 449–476.
[43] Nathaniel Fruchter and Ilaria Liccardi. 2018. Consumer attitudes towards privacy and security in home assistants. In *Proceedings of the 2018 ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–6.
[44] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. 2019. The Effect of Entertainment Media on Mental Models of Computer Security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, USA, 79–95. https://www.usenix.org/conference/soups2019/presentation/fulton.
[45] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–12.
[46] Nina Gerber and Karola Marky. 2022. The Nerd Factor: The Potential of S&P Adepts to Serve as a Social Resource in the User's Quest for More Secure and Privacy-Preserving Behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Usenix, Berkely, CA, USA, 57–76.
[47] Iwan Gulenko. 2014. Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security* 22, 2 (2014), 167–178.
[48] Ken H Guo, Yufei Yuan, Norman P Archer, and Catherine E Connelly. 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems* 28, 2 (2011), 203–236.
[49] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the 2014 ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 2647–2656.
[50] Tejaswini Herath and H Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems* 18, 2 (2009), 106–125.
[51] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A world full of privacy and security (mis) conceptions? Findings of a representative survey in 12 countries. In *Proceedings of the 2023 ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–23.
[52] Qing Hu, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences* 43, 4 (2012), 615–660.
[53] IBM Security. 2024. Cost of a Data Breach Report 2024. https://www.ibm.com/security/data-breach Accessed: 2024-09-06.
[54] Princely Ifinedo. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management* 51, 1 (2014), 69–79.
[55] Alice M. Isen. 1984. Toward Understanding the Role of Affect in Cognition. In *Handbook of Social Cognition*, Robert R. Wyer and Thomas K. Srull (Eds.). Vol. 3. Lawrence Erlbaum Associates, Mahwah, NJ, 179–236.
[56] Philip Nicholas Johnson-Laird. 1995. *Mental models: Towards a cognitive science of language, inference, and consciousness* (6. print ed.). Cognitive science series, Vol. 6. Harvard Univ. Press, Cambridge.
[57] Allen C Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: An empirical study. *MIS quarterly* 34, 3 (2010), 549–566.
[58] Natalie A. Jones, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch. 2011. Mental Models: An Interdisciplinary Synthesis of Theory and Methods. *Ecology and Society* 16, 1 (2011), 1–13. http://www.jstor.org/stable/26268859
[59] Yi Xuan Khoo, Rachael M Kang, Tera L Reynolds, and Helena M Mentis. 2024. "That's Kind of Sus (picious)": The Comprehensiveness of Mental Health Application Users' Privacy and Security Concerns. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–16.
[60] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 246–263. https://doi.org/10.1109/SP.2019.00060
[61] Isadora Krsek, Kimi Wenzel, Sauvik Das, Jason I. Hong, and Laura Dabbish. 2022. To Self-Persuade or be Persuaded: Examining Interventions for Users' Privacy Setting Selection. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 623, 17 pages. https:

//doi.org/10.1145/3491102.3502009

[62] Evan Lafontaine, Aafaq Sabir, and Anupam Das. 2021. Understanding people's attitude and concerns towards adopting IoT devices. In *Proceedings of the 2021 ACM CHI Conference on Human Factors in Computing Systems - Extended Abstracts*. ACM, New York, NY, USA, 1–10.

[63] Charles G Lord, Sarah E Hill, Christopher J Holland, Kristin Yoke, and Tong Lu. 2015. Attitudes: An evolutionary perspective. In *Evolutionary perspectives on social psychology*. Springer, New York, NY, 177–187.

[64] Patricia J Manney. 2008. Empathy in the Time of Technology: How Storytelling is the Key to Empathy. *Journal of Evolution & Technology* 19, 1 (2008), 1–11.

[65] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, and Imogen Verret. 2022. Why IT Security Needs Therapy. In *Computer Security. ESORICS 2021 International Workshops (Springer eBook Collection)*, Sokratis Katsikas, Costas Lambrinoudakis, Nora Cuppens, John Mylopoulos, Christos Kalloniatis, Weizhi Meng, Steven Furnell, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, and Marco Antonio Sotelo Monge (Eds.). Springer International Publishing and Imprint Springer, Cham, 335–356. https://doi.org/10.1007/978-3-030-95484-0{_}20

[66] Lachlan Moore, Tatsuya Mori, and Ayako A Hasegawa. 2024. Negative Effects of Social Triggers on User Security and Privacy Behaviors. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Usenix, Berkely, CA, USA, 605–622.

[67] Robin L Nabi and Melanie C Green. 2015. The role of a narrative's emotional flow in promoting persuasive outcomes. *Media Psychology* 18, 2 (2015), 137–162.

[68] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 2021. A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In *Proceedings of the 30th USENIX Security Symposium*. USENIX Association, Berkeley, CA, 1235–1252. https://www.usenix.org/conference/usenixsecurity21/presentation/huaman

[69] Donald A Norman. 2014. Some observations on mental models. In *Mental models*. Psychology Press, Los Altos, CA, 15–22.

[70] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security* 66 (2017), 40–51.

[71] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: Stories as Informal Lessons about Security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, USA, 1–18. https://www.usenix.org/conference/soups2022/presentation/pfeffer.

[72] Radmila Prislin and Wendy Wood. 2014. Social Influence in Attitudes and Attitude Change: the Role of Social Consensus on Attitudes and Attitude Change. In *Handbook of Attitudes*, Dolores Albarracín, Blair T. Johnson, and Mark P. Zanna (Eds.). Psychology Press, Mahwah, NJ, US, 671 – 706.

[73] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 6, 17 pages. https://doi.org/10.1145/2335356.2335364

[74] Maike M. Raphael, Aikaterini Kanta, Rico Seebonn, Markus Dürmuth, and Camille Cobb. 2024. Batman Hacked My Password: A Subtitle-Based Analysis of Password Depiction in Movies. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 199–218. https://www.usenix.org/conference/soups2024/presentation/raphael

[75] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[76] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, 272–288. https://doi.org/10.1109/sp.2016.24

[77] Dennis T Regan and Russell Fazio. 1977. On the consistency between attitudes and behavior: Look to the method of attitude formation. *Journal of experimental social psychology* 13, 1 (1977), 28–45.

[78] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the new security paradigms workshop*. ACM, New York, NY, USA, 42–56.

[79] Karen Renaud, Rosalind Searle, and Marc Dupuis. 2021. Shame in cyber security: effective behavior modification tool or counterproductive foil?. In *Proceedings of the 2021 New Security Paradigms Workshop*. ACM, New York, NY, USA, 70–87.

[80] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. 2021. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications* 8, 1 (2021), 1–17.

[81] J Edward Russo, Paul JH Schoemaker, et al. 1992. Managing overconfidence. *Sloan management review* 33, 2 (1992), 7–17.

[82] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78.

[83] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. 2016. Information security policy compliance model in organizations. *computers & security* 56 (2016), 70–82.

[84] M. A. Sasse and I. Flechais. 2005. *Usable Security: Why Do We Need It? How Do We Get It?* O'Reilly, Sebastopol, US. https://discovery.ucl.ac.uk/id/eprint/20345/

[85] Lorin Schöni, Victor Carles, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. 2024. You Know What? - Evaluation of a Personalised Phishing Training Based on Users' Phishing Knowledge and Detection Skills. In *Proceedings of the 2024 European Symposium on Usable Security*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3688459.3688460

[86] Pavel Seda, Jan Vykopal, Valdemar Švábenský, and Pavel Čeleda. 2021. Reinforcing Cybersecurity Hands-on Training With Adaptive Learning. In *2021 IEEE Frontiers in Education Conference (FIE)*. IEEE, New York, NY, USA, 1–9. https://doi.org/10.1109/FIE49875.2021.9637252 ISSN: 2377-634X.

[87] James Shires. 2020. Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy* 41, 1 (2020), 82–107.

[88] Mario Silic and Paul Benjamin Lowry. 2020. Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems* 37, 1 (2020), 129–161.

[89] Mikko Siponen, M Adam Mahmood, and Seppo Pahnila. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & management* 51, 2 (2014), 217–224.

[90] Paul C Stern, Linda Kalof, Thomas Dietz, and Gregory A Guagnano. 1995. Values, beliefs, and proenvironmental action: Attitude formation toward emergent attitude objects 1. *Journal of applied social psychology* 25, 18 (1995), 1611–1636.

[91] Johan Svenningsson, Gunnar Höst, Magnus Hultén, and Jonas Hallström. 2022. Students' attitudes toward technology: exploring the relationship among affective, cognitive and behavioral components of the attitude construct. *International Journal of Technology and Design Education* 32, 3 (2022), 1531–1551.

[92] Gesa Van den Broek, Atsuko Takashima, Carola Wiklund-Hörnqvist, Linnea Karlsson Wirebring, Eliane Segers, Ludo Verhoeven, and Lars Nyberg. 2016. Neurocognitive mechanisms of the "testing effect": A review. *Trends in Neuroscience and Education* 5, 2 (2016), 52–66.

[93] Roxanne I van Giesen, Arnout RH Fischer, Heleen van Dijk, and Hans CM van Trijp. 2015. Affect and cognition in attitude formation toward familiar and unfamiliar attitude objects. *PloS one* 10, 10 (2015), e0141790.

[94] Kami E Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the ACM CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 2671–2674.

[95] Melanie Volkamer and Karen Renaud. 2013. Mental models–general introduction and review of their application to human-centred security. In *Number theory and cryptography: Papers in honor of johannes buchmann on the occasion of his 60th birthday*. Springer, Berlin, Heidelberg, 255–280.

[96] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing simulated phishing campaigns for staff. In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25*. Springer, Guildford, UK, 312–328.

[97] Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. 2024. Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 623–642. https://www.usenix.org/conference/soups2024/presentation/von-preuschen

[98] Alexandra von Preuschen, Verena Zimmermann, and Monika C Schuhmacher. 2023. How do you Feel about Cybersecurity?–A Literature Review on Emotions in Cybersecurity. In *International Symposium on Technikpsychologie (TecPsy) 2023*. Sciendo, Darmstadt, Germany, 1–13.

[99] Serena Wang, Cori Faklaris, Junchao Lin, Laura Dabbish, and Jason I. Hong. 2022. 'It's Problematic but I'm not Concerned': University Perspectives on Account Sharing. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1, Article 68 (April 2022), 27 pages. https://doi.org/10.1145/3512915

[100] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, New York, NY, USA, 1–16.

[101] Neil D Weinstein. 1980. Unrealistic optimism about future life events. *Journal of personality and social psychology* 39, 5 (1980), 806.

[102] Lisa A Williams and David DeSteno. 2008. Pride and perseverance: the motivational role of pride. *Journal of personality and social psychology* 94, 6 (2008), 1007.

[103] Gordon Winocur and Morris Moscovitch. 2011. Memory transformation and systems consolidation. *Journal of the International Neuropsychological Society* 17, 5 (2011), 766–780.

[104] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 395–409. https://www.usenix.org/conference/soups2018/presentation/wu

[105] Chul Woo Yoo, Jahyun Goo, and H. Raghav Rao. 2020. Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. *MIS Quarterly* 44, 2 (2020), 907–931. https://doi.org/10.25300/MISQ/2020/15477

[106] Fatemeh Mariam Zahedi, Yan Chen, and Huimin Zhao. 2023. Ontology-Based Intelligent Interface Personalization for Protection Against Phishing Attacks. *Information Systems Research* 35, 3 (Oct. 2023), 1463–1478. https://doi.org/10.1287/isre.2021.0065

[107] Mark P. Zanna and John K. Rempel. 2008. Attitudes: A new look at an old concept. In *Attitudes: Their structure, function, and consequences*. Psychology Press, New York, NY, US, 7–15.

[108] Verena Zimmermann and Karen Renaud. 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies* 131 (2019), 169–187.

A Appendices

A.1 Interview Guide

(1) To help you fully immerse yourself in our interview, I'm going to take you on a journey. If you'd like, feel free to close your eyes to better visualize the situation. Imagine you are at your workplace in the office. Take your time—you've just arrived and are looking around [short pause]. I'll wait for a signal from you once you've settled in [short pause].
Now you start your workday, open your laptop, and begin working. You open your email inbox and see an email from management. The email states that cybersecurity is now one of the company's top priorities.
a. When you think of the word "cybersecurity" in this environment, what thoughts come to mind?
b. Do certain images come to mind? What exactly do you see?
c. Briefly describe these images to me.
(2) In this study, "cybersecurity" is defined as follows: Cybersecurity is the protection of the electronic organizational network, electronically transmitted data and information, the protection of the transmission medium, as well as the protection of processes, workflows, and end-users.
a. How do you perceive cybersecurity in your daily work?
b. What is your attitude toward cybersecurity in your daily work?
c. Where do you think this attitude comes from?
d. What priority do you assign to cybersecurity and why?
e. What priority does your company assign to cybersecurity?
(3) How do you think your attitude towards cybersecurity affects your corresponding behavior?
(4) How do you handle cybersecurity measures in your daily work? Feel free to mention specific examples.
(5) Is there a contact point for cybersecurity concerns in your company?
(6) In your opinion, how should cybersecurity measures be designed?
(7) What measures do you think are necessary to develop a positive perception of cybersecurity?

A.2 Focus Group: Tasks

Starting Point: Cybersecurity is declared one of the top priorities of the business department. Each department is to establish its own cybersecurity strategy. What measures or framework conditions are necessary for you to optimally adapt your work behavior to this? What can support you in culturally establishing a positive attitude toward cybersecurity? Please follow Step 1 first, then Step 2 in your response.

(1) Brainstorming: First, spend 10 minutes brainstorming and collecting your thoughts on this. You can use elements from the toolbox on Slide 2 to help.
(2) Work phase: After the brainstorming session, it's time to move on to the main work phase. Please create a model, diagram, or overview with text and optionally with icons to answer the above task. Use the icon box on Slide 4 for additional inspiration. Remove the transparent box on Slide 4 so you can see the icons. Make sure your presentation is self-explanatory. You have 20 minutes. After that, you will present your results.

A.3 Definitions of (Sub)themes

The codebook includes definitions of the subthemes. For exemplary quotes, please refer to the respective visualization within the result section.

Theme	Subtheme	Definition
		RQ1
Affective Component	valence	Perception of a stimulus on a range from pleasant to unpleasant
	arousal	State of emotional or physical energy that influences an individual's response to stimuli ranging from low to high
Cognitive Component	Narrative	Overarching story, perspective, or framing used by individuals to describe cybersecurity
	Complexity and abstraction	Extent to which individuals view cybersecurity as difficult to understand or detached
	Importance and necessity	Individual's subjective evaluation of how critical and essential cybersecurity is
Conative Component	Awareness and caution	recognition and understanding of one's environment and circumstances related to potential threats; careful consideration of one's actions
	Supportive behavior	Proactive engagement concerning cybersecurity-related actions
	Procrastination	Act of delaying or postponing tasks despite knowing potential unfavorable outcomes
	Avoidance	Deliberately staying away from aspects related to cybersecurity
	Minimal Effort	Tendency to engage in the least amount of action or investment required
		RQ2
Past	direct	Prior experiences that an individual has gone through themselves
	indirect	Retrievals from statements regarding others' past experiences
Ongoing	direct	Continuous experiences that an individual creates for themselves
	indirect	Retrievals from statements regarding others' continuous experiences
Future	direct	Expectations about the future that an individual creates for themselves
	indirect	Retrievals from statements regarding others' future expectations
Individual factors	Level of perceived vulnerability	An individual's personal evaluation of their likelihood of experiencing harm or risk.
	Level of knowledge	depth and breadth of understanding an individual has
	Perceived distance	An individual's sense of disconnection or lack of connection
	Experienced knowledge-behavior gap	Experienced discrepancy between what individuals know based and their actual behaviors
	Perceived level of data sensitivity	Individual's subjective judgment about the importance, confidentiality, and potential risks associated with specific data
	Perceived security culture	Individual's understanding and interpretation of the shared values, and practices within an organization concerning security

Theme	Subtheme	Definition
	RQ3	
Social and cultural framework	Management security actions	Strategies, decisions, and actions taken by an organization's management to address cybersecurity-related issues
	Social acceptance	Process by which individuals or groups are recognized, included, and regarded positively concerning security related actions within a social context
	User-Inclusion in Cybersecurity processes	Active involvement of users in the design, development, and decision-making processes of cybersecurity related issues
	Team security vision	Shared, overarching security goal that aligns and motivates team members, providing direction and a sense of collective purpose
	Security Decision Autonomy	Ability to make independent security-related decisions
	Security as a Process	continuous and adaptive implementation of measures and behaviors tailored to the stage's needs
	Technical framework and infrastructure	Underlying systems, tools, and structures that support and enable technical solutions
Communication style	Security Simplicity and Usability	User-friendliness and straightforwardness of security processes and interfaces
	Positive Security Mindset	Practice of focusing on the good aspects of security situations (e.g., what already goes well) and implementing an optimistic stance
	Security tangibility and branding	Physical and perceivable elements that reinforce a brand's identity
	Transparent security actions and communications	Practice of being open and clear in communication and actions about security
Education contents	Security knowledge enhancement and transfer	Process of improving and sharing security knowledge to promote learning
	Security scenarios and Stories	Narratives or description of security-related situations to convey messages
	Support for Security-related self-reflection	Process of examining one's thoughts, feelings, and behavior concerning cybersecurity
	Organizational cybersecurity strategy	Plan designed to protect an organization
Educational formats	Type of Security Learning Format	Specific method or structure of learning formats for cybersecurity related contents
	Frequency of security education	Rate of occurence of security education

Table 3: Definitions of (sub)themes

A.4 Results from the focus groups (working phase)

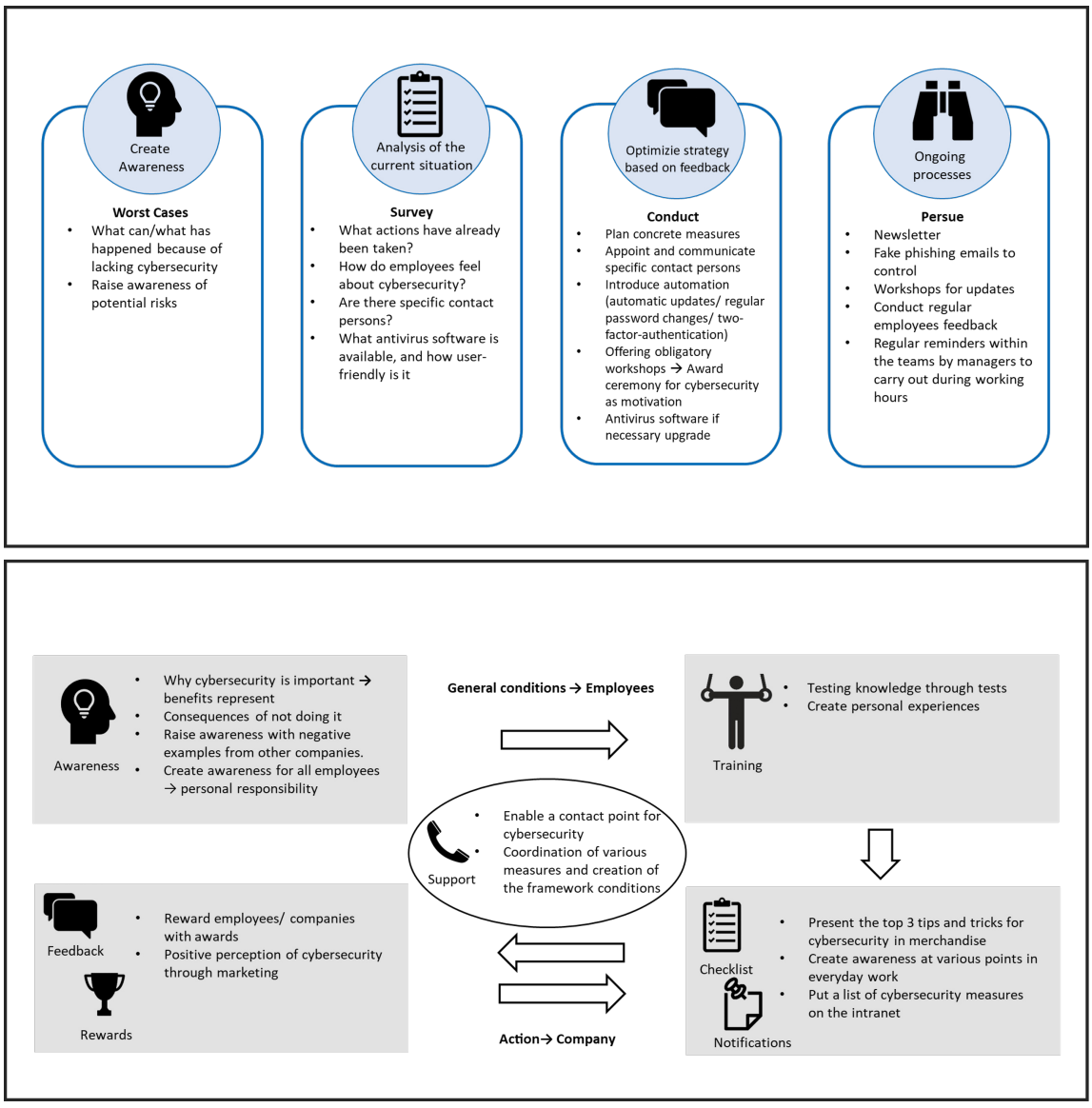


Figure 7: Results from two of the four focus groups from the working phase. Since some group names provide information about the department of the participants, no group names are given in order to protect the privacy of the participants. (2/4)

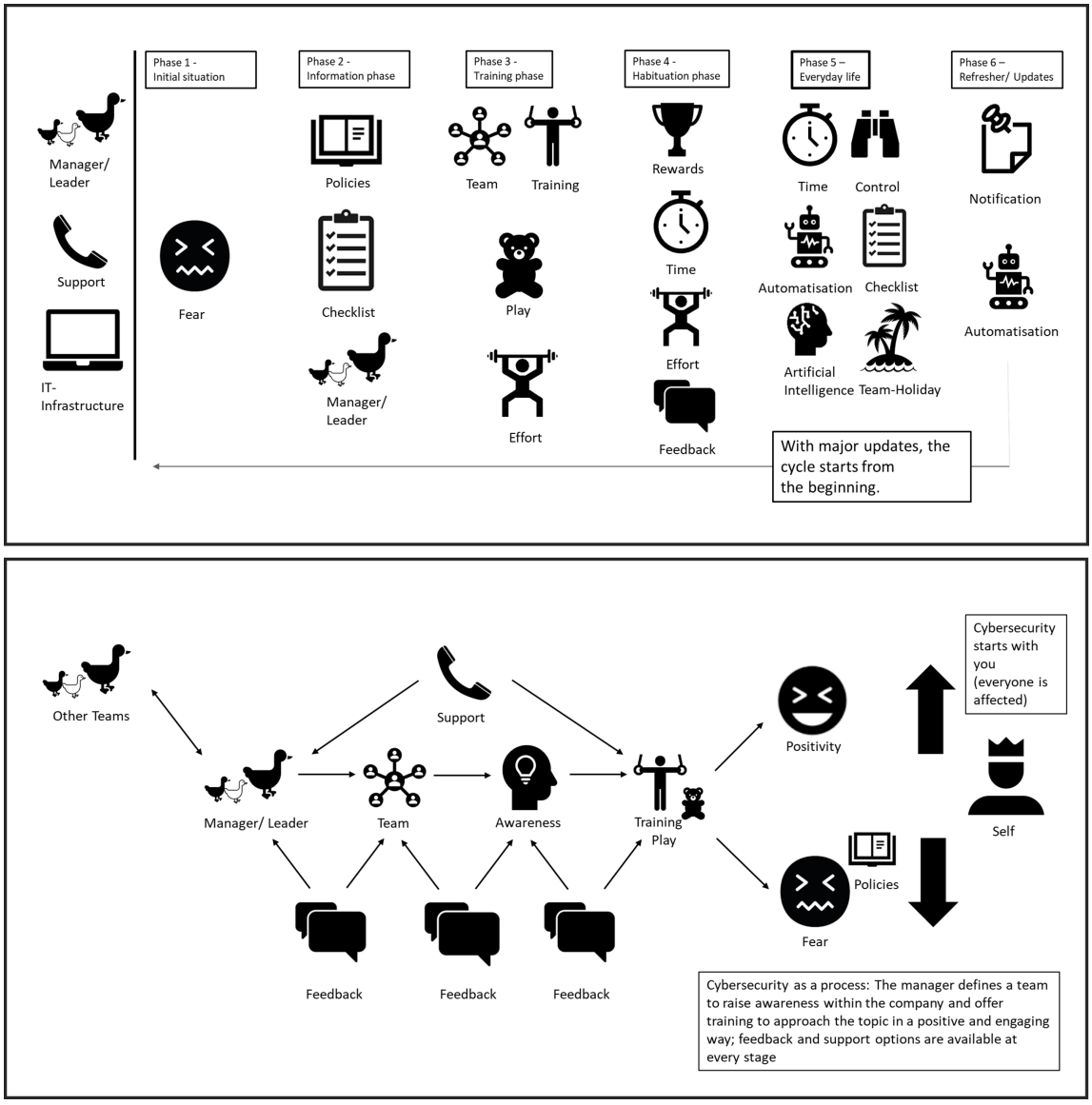


Figure 8: Results from two of the four focus groups from the working phase. Since some group names provide information about the department of the participants, no group names are given in order to protect the privacy of the participants. (4/4)

Chapter 6

Paper D: Emotions as a Method to Extend Cybersecurity Frameworks with a Human-centered Lens

The paper was published as follows:

Alexandra von Preuschen, Roman Henke, Manpreet Kaur, Julian Nickel, and Monika C. Schuhmacher. 2025, in press. Towards an Employee-Centric Framework of Cybersecurity. In European Symposium on Usable Security (EuroUSEC 2025), Manchester, UK.

Towards an Employee-Centric Framework of Cybersecurity

Alexandra von Preuschen, Roman Henke, Manpreet Kaur, Julian Nickel and Monika C. Schuhmacher
Justus-Liebig-University
Giessen, Germany
Email: alexandra.vonpreuschen@wirtschaft.uni-giessen.de

***Abstract*—While the critical role of employees in cybersecurity has long been recognized, there is a lack of a comprehensive and holistic understanding regarding the key points of contact of employees with cybersecurity, beyond mere preventive actions. To address this gap, we conducted an exploration of key points of contact between employees and cybersecurity using semi-structured interviews (n = 20) and identified employee aspects within the functions of the NIST Cybersecurity Framework (NIST-CSF). We demonstrate that particular perceptions, emotions, and social dynamics are relevant to employees' perspectives on cybersecurity in comparison to the rather technical inclusion of the employees within the NIST-CSF.**

By aligning the employees' perspectives with the functions/subcategories of the NIST-CSF, we take a step towards an employee-centric framework for cybersecurity that highlights these essential key points of contact between employees and cybersecurity and points out gaps for the integration of employees in organizational cybersecurity. We conclude the paper by giving recommendations for practitioners and future research.

***Index Terms*—organizational cybersecurity, employee-cybersecurity touchpoints, framework, qualitative**

I. Introduction

Research has investigated the integration of employees in organizational cybersecurity for decades, underscoring their critical role in both enabling and hindering favorable security outcomes [1], [2]. Despite the ongoing debate on the role of employees in organizational cybersecurity, promoting secure employee behavior remains a challenge [3], [4]. This suggests that current cybersecurity frameworks may not fully grasp or address the complex interplay between humans and technological aspects, potentially missing out on essential aspects that might influence security behavior or cybersecurity in general. Most existing cybersecurity frameworks, such as the NIST Cybersecurity Framework (NIST-CSF), are fundamentally structured from the standpoint of professionals, prioritizing policies and practices that manage risks [5]. Although they adeptly define core activities like protection, these frameworks marginally address the dynamic interactions employees have with security — often reducing their role to mere compliance and viewing training within the "Protect" function.

Similarly, most literature that explores the promotion of positive cybersecurity behavior tends to focus on preventive measures and compliance [6], with only some articles highlighting the significant impact of other factors, such as experiencing a cybersecurity incident on cybersecurity behavior [7], [8].

This suggests that the key points of contact between employees and cybersecurity in their daily work are not well-documented, which underscores the need to holistically identify the key points of contact between employees and cybersecurity. Points of contact here refer to specific moments or elements in daily work, interactions where employees actively or passively engage with cybersecurity.

Consequently, our research paper aims to take a first step towards an employee-centric framework of cybersecurity that considers key points of contact between employees and security, as well as their perspectives on cybersecurity.

To gain a deeper understanding of how employees interact with organizational cybersecurity, we analyzed employee-related aspects of the NIST-CSF [5] and conducted semi-structured interviews (n = 20) on emotions-invoking elements within the functions of the NIST-CSF to identify key points of contact from an employee's perspective (please view the methods section for an explanation of our approach). Finally, we identified employee aspects within the functions of the NIST-CSF and then mapped these to the results from the interviews for an employee-centric framework of cybersecurity.

The contributions of the study are three-fold:

1) We take a step towards an employee-centric framework of cybersecurity that combines NIST-CSF principles with an employee perspective that can be implemented by practitioners and researchers. For employees, we provide a framework to support them in identifying their role within cybersecurity.
2) We uncover key points of contact between employees and cybersecurity that drive employee engagement with/distancing from security.
3) We identify gaps in the integration of employees into organizational cybersecurity.

II. Related Work

Cybersecurity represents a complex field characterized by a range of interpretations of the term. The National Institute of Standards and Technology (NIST) presents multiple definitions within its glossary, outlining that cybersecurity describes a process focused on the protection of information in cyberspace that includes prevention, detection, and responding to cyber threats [9]–[11]. Another definition provided emphasizes the necessity of establishing measures to protect electronic information and communication systems and the data they contain,

securing them against harm, exploitation, and unauthorized use [12].

Recent literature has increasingly investigated human aspects in cybersecurity, marking a shift from the traditional focus that prioritized technical factors while often neglecting human-related aspects [1], [13], [14]. In predominant research, the human element is typically cast as the weakest link in cybersecurity, a view supported by literature indicating that human error prominently leads to system threats [14], [15]. As a result, attempts are often made to counteract human error by implementing stringent safety protocols or restricted system access, stemming from the notion that no system is immune to human fallacy [1]. However, it is crucial to understand human aspects and behavior within the context of cybersecurity and incorporate this understanding into security models, as this could significantly diminish the "human risk" and thereby strengthen organizational cybersecurity [1], [16]. Strengthening the human factor, instead of protecting organizations solely with technical solutions, can enhance defense against cybercriminals who often exploit human behaviors [17]. Thus, a human-centric perspective on cybersecurity is crucial, requiring a comprehensive understanding of humans and their integration as a key component of security systems [1], [2], [18]. Moreover, Zimmermann and Renaud advocate for rethinking cybersecurity in terms of "cybersecurity differently," in which humans should be acknowledged as contributors to cybersecurity, not just as a problem [1]. Their research indicates that while traditionally, human behavior has been extensively studied as a source of problems, their role within cybersecurity has not been sufficiently explored. Instead of trying to control human behavior, it is important to view humans as contributors to better cybersecurity resilience who can prevent and detect potential threats [1].

However, despite growing recognition of the human element in cybersecurity, foundational frameworks such as the NIST-CSF only marginally address employees' role within cybersecurity, emphasizing technical interaction over psychological aspects of interactions. The NIST-CSF in version 1.1 outlines five core functions to systematically structure cybersecurity risk management: Identify, Protect, Detect, Respond, and Recover [5]. In NIST-CSF version 2.0, a new function called Govern was added. These functions guide organizations through recognizing assets and risks, ensuring their protection, detecting incidents, responding to breaches, and restoring normal operations.

Building on these core functions, the framework is further subdivided into categories and subcategories. Although some subcategories reference the human factor, employees are recognized primarily as operational actors tasked with training (PR.AT-1), access management (PR.AC-1), and incident response duties (RS.CO-1) [5]. Thus, the role of employees is primarily conceptualized around compliance and technical adherence, with little attention to the broader psychological, social, and emotional factors that shape security behavior [6], [16]. Employees are positioned as passive recipients of policies rather than proactive stakeholders whose experiences contribute to cybersecurity resilience.

Furthermore, the framework implicitly treats employees as rational decision-makers who will reliably execute prescribed actions once roles and procedures are defined, for example, in RS.CO-1, which states that "personnel know their roles and order of operations when a response is needed." However, this assumption neglects the reality that employees, like all decision-makers, operate under bounded rationality [19] and are subject to cognitive limitations [20] and emotional pressures that can impair their ability to act as intended during cybersecurity incidents.

Recent studies show that cybersecurity behavior is much influenced by emotional aspects, including fear, shame, frustration, and pride [7], [21]. Emotional reactions to demanding password regulations or extensive and complex policies, for instance, might cause resistance, circumventions, or emotional weariness. Yet, the NIST-CSF is lacking the integration of these emotional or experience dynamics. Therefore, even if the framework provides thorough technical direction, it only marginally touches upon human aspects.

Following this observation, Rohan et al. [22] mapped 20 human factors and 12 security practices, derived from a literature review, to the NIST-CSF, finding that only Protect, Detect, and Respond functions incorporate human aspects (e.g., awareness, behavior, and attitude) while Identify and Recover remain largely technical. The authors argue that this is due to the function's technical and procedural nature, which involves minimal human participation and mostly follows set procedures. While this work makes progress in identifying human aspects within NIST-CSF, it is limited to a top-down mapping approach, which constrains human factors within predetermined technical framework categories rather than exploring the full spectrum of employee experiences with cybersecurity. Thus, our work seeks to advance this field by incorporating both passive and active key points of contact between employees and organizational cybersecurity, going beyond established practices, and integrating employee perspectives.

III. Method

To identify key points of contact and an employee's perspective, we used two data streams:

1) We presented employees with the functions from the NIST-CSF by conducting **semi-structured interviews** with 20 participants. As asking employees to share their emotional experiences related to cybersecurity events can facilitate better recollection with more vivid and accurate memories - allowing for deeper insights that go beyond just the factual details than merely asking them to recall what happened [23], [24] - we used emotions as a way to understand key points of contact (emotion-evoking aspects of cybersecurity) that impact employees daily.
2) We identified **key points of contact within the NIST-CSF** by identifying employee aspects within the functions of the NIST-CSF (version 1.1). For this, we first

mapped findings from the interviews to the rewritten NIST-CSF subcategories and identified those subcategories from the NIST-CSF that were not mentioned in the interviews.

A. Interview

The following section outlines the study procedure, sample details, ethical considerations, and our approach to data analysis.

1) Participants: To ensure a diverse sample, the recruitment approach involved interviewing individuals of various ages, job positions, industries, backgrounds, and levels of IT and cybersecurity knowledge. Employees were contacted through email, social media platforms word-of-mouth, personal connections, and snowballing. The study sample consists of German 20 participants (two of them currently residing in Canada), with 60% identifying as women (12 individuals) and 40% as men (8 individuals), aged between 20 and 54. Participants from 16 industries have one to over 21 years of experience. To gain a deeper understanding of our sample and to control for variations in IT expertise and security expertise, we included a five-point scale ranging from 1 (low) to 5 (high) for participants to rate both areas.Their self-rated IT expertise averages M=4.65 (SD=0.93) and cybersecurity expertise M=3.70 (SD=1.30). Seventeen reported cybersecurity was not a primary job aspect, two did, and one mentioned recruiting Chief Information Security Officers. Interviews concluded at data saturation.

2) Study Procedure: The data was derived from a more extensive interview study conducted in April 2024 that aimed to explore emotional experiences, building on the findings of von Preuschen et al. [21]. In line with this approach, we defined the scope of our study to focus specifically on emotional experiences within the established framework. Given the ongoing nature of the broader study, we have carefully selected specific data segments that align with our research objective. These segments provide valuable context for understanding employee interactions with cybersecurity key points of contact. This section outlines the relevant steps for this work taken from the broader study:

Pre-interview survey. One to two weeks before the interview, participants completed a screening survey for informed consent and demographic information while selecting a code for anonymity. The survey included the short version of the Job-related Affective Well-being Scale [25], [26], which assesses employees' emotional well-being and job satisfaction by measuring positive (e.g., happiness) and negative (e.g., anger) affects at work.

In the next step, to further assess the cybersecurity climate within their respective organization the Information Security Climate Index was employed [27], a tool used to evaluate how information security is perceived and understood within a company. For comprehensive screening details, please refer to Appendix A. Following these two scales, we presented the functions from the NIST-CSF, emphasizing the human aspects. Lastly, the interviewees were instructed to reflect on the following question before the upcoming interview: "What experiences do I have with cybersecurity in my day-to-day work?".

Interviews. The interviews were conducted remotely using a video conference tool. Participants were given the choice to activate or deactivate their cameras throughout the duration of the interviews. The interviews were recorded in audio format with the participants' consent and transcribed using Microsoft Word. Any inaccuracies in the transcriptions were corrected manually by cross-referencing with the audio recordings to ensure accurate and smoothed transcription. Participants were welcomed and thanked for their involvement. Consent was verified both for participation and audio recording. They were informed about the interview duration (approximately one hour), the sensitive nature of the topic, and the confidentiality of their data. To create a comfortable and secure environment, participants were assured that there were no right or wrong answers, encouraging genuine and reflective responses. They were given time to process questions and were reminded of the key survey areas. Assistance was offered in articulating emotions. The interview began after addressing any remaining questions. A digital whiteboard (Miro) was used via screen sharing to document details and display the NIST-CSF functions throughout the discussion. The interview itself was structured as following:

- **Warm-up: Cybersecurity and associated emotions.** To build a common understanding of cybersecurity, participants first shared three terms or definitions related to organizational cybersecurity. The study's definition of cybersecurity was then presented. Next, to slowly approach emotional topics and emotion-evoking events, representing key points of contact of employees with cybersecurity, participants identified and discussed emotions evoked by cybersecurity. Following the procedure outlined in [21], participants utilized the non-verbal PrEmo tool [28], [29] to select cartoon characters that represented their emotional states. After reflecting on and labeling these emotions, participants reviewed a list of 65 cybersecurity-related emotions from [21] and identified additional emotions that resonated with them.
- **Experiences and emotions towards key points of contact with cybersecurity.** Participants were reminded of the survey and the key points of contact with cybersecurity. They shared their reflection on their cybersecurity experiences and consecutive emotions. Ample time was provided, and they could explore the NIST-CSF functions further or share specific memories. Follow-up questions addressed the impact on their behavior and organizational culture.

3) Ethical considerations: In our institution, there is no formal IRB process available for this type of study. Nevertheless, it is the duty of the researchers and their supervisors to consider and ensure compliance with ethical and legal standards. Participants provided written consent detailing the study's nature. It was specifically emphasized that participation was

voluntary, and the participants were informed of their right to withdraw at any time without facing any consequences. Before the interviews, they received explanations about data handling, including audio recording and transcript storage, ensuring confidentiality. Only essential personal data was collected, with age categorized abstractly, and participants created personal codes for identity protection. Data was securely stored per national laws, and support was offered for discomfort or strong emotional reactions, including breaks during interviews. The study prioritized privacy and well-being, adhering to ethical guidelines and fostering open dialogue to enhance the credibility of its outcomes.

4) Data Analysis: Thematic analysis according to Braun and Clarke was employed for the analysis of the transcribed data [30]. The thematic analysis was carried out following the guidelines of Braun and Clark by first reading through all completed transcripts multiple times. Subsequently, four transcripts were randomly chosen for coding at the sentence level, leading to the development of an initial codebook, which was continuously discussed and refined with a fellow researcher. This iterative process was then replicated with the remaining transcripts until all had been coded and potential themes had been identified. Following the completion of an initial codebook that included potential themes, a thorough review of all data was conducted to validate the codes and implement any required modifications. This validation process was repeated three times until a final codebook was created, in which the final themes were grouped together.

B. Identification of employees' key points of contact within the NIST-CSF functions.

We reviewed all subcategories of the NIST-CSF and identified potential key points of contact with employees (see Appendix C). We then identified where employees may have contact with cybersecurity. Lastly, we mapped these with the themes identified through the interviews to establish a final framework.

IV. Results: Interviews

The interview's results are organized by themes, with quotes included as needed. Due to the exploratory nature of the study, specific numbers are excluded in favor of frequency ranges to avoid assumptions of generalizability, consistent with previous research [31].

This section revolves around the experiences that participants have had with organizational cybersecurity, which were shared according to the functions of cybersecurity according to the NIST-CSF: Identify, Protect, Detect, Respond, and Recover.

A. Identify

A common theme across many interviews is the recognition of institutional regulations that are designed to support effective cybersecurity management.

Awareness of Key Contacts. Many participants acknowledged the existence of designated contact persons for cybersecurity matters, such as data protection officers or IT departments. These individuals are actively involved in ensuring compliance with cybersecurity measures and raising awareness among employees. For instance, one participant noted,

> *"We have a department called [name of department...] and as far as I know, it's the department responsible for all IT, e.g., cybersecurity issues. Furthermore, this department also serves as the first point of contact."* (P5).

Another participant referred to his appreciation of regular communication:

> *"We also keep receiving emails, which I find very effective, containing all the contact details."* (P11).

In contrast, some participants expressed a lack of awareness about their cybersecurity contacts, as highlighted by another participant's remark (P14):

> *"...about this data security officer, I didn't even know that we had one, nor do I know what exactly his tasks are"*.

This varied awareness of key contacts underscores a deficiency in communication tactics within the organization. While there is some research on security experts and security experts and their dynamics with users [32], [33], there is limited exploration of the availability of security support and the methods of delivering it.

Policy Awareness. Participants frequently cited the existence of clear policies and procedures as a fundamental element of organizational cybersecurity. However, the level of awareness and understanding of these policies varied considerably, with some participants feeling well-informed while others were only vaguely aware of their existence (P16, P12, P18).

While security awareness has been a longstanding key construct, there is a plethora of literature highlighting why security awareness alone often fails to change behavior [4]. Most research primarily examines security awareness without considering awareness of company-specific policies [34]. Other studies measure the intention to comply with/intention to violate policies without actually assessing whether users are aware of the content of them [35].

B. Protect: Preventive Measures

Participants frequently mentioned the strict adherence to security protocols such as password updates and encryption of sensitive data, as well as identity and access management, which determines the authentication procedures utilized. Literature often focuses on preventive measures, highlighting various aspects such as password choices or caution with potentially malicious content in emails [6].

Regular Password Changes. Most participants noted strict adherence to security protocols, particularly regarding passwords. They described that they are required to create strong passwords (P15) and change them regularly (e.g., P10). Further, participants mentioned that they are urged to under-

take this action through regular reminders (P11). Despite the widespread adoption of this practice within organizations, the sentiments expressed by nearly all participants leaned towards irritation and annoyance at having to do this at regular intervals (e.g., P5). This is particularly evident in the case of one participant (P6):

> *" I think [passwords] had to be changed almost every 8 or 10 weeks, which, when I think of myself now, was a huge source of frustration. Annoyance, because at some point I couldn't remember my passwords anymore. So, I started writing them down, which is actually exactly the opposite effect. I wrote them down somewhere and still forgot the password, which meant that after the third incorrect entry my system was locked and I had to call a hotline to unlock it, but I was 3 minutes before a client call and arrived too late in a call where I was expected."*

However, numerous individuals have articulated their comprehension of the necessity to engage in this practice after receiving sufficient awareness by their organizations, with some even asserting that it contributes to their sense of security, regardless of the annoyance felt in the previously mentioned scenarios (P12). Our findings build on previous research: Although feelings of annoyance and frustration align with earlier studies' recommendations against frequent password changes [2], our results also reveal a sense of security when such changes are implemented.

Use of Multi-factor Authentication. Many participants noted the daily use of multi-factor authentication as a security measure. This protocol is seen as an effective addition (P4) and is considered more user-friendly than constantly remembering new passwords (P15). This aligns with previous research suggesting for organizations to enhance cyber hygiene by adopting user-friendly measures like two-factor authentication to boost employee engagement in security tasks [36], [37]. However, some expressed frustration (P7) with the need to re-authenticate after periods of inactivity (P10).

Data Encryption. Another frequently mentioned preventive measure was the encryption of emails and other data, especially those containing sensitive information (P16). This practice is part of a policy aimed at protecting data from unauthorized access (P6). Hereby, the majority indicated their support for this practice, citing their awareness of the sensitivity of the data.

C. Protect: Awareness and Training

Training offering. The participants commonly reported the presence of cybersecurity awareness training programs within the organizations, some of which were mandatory for them to participate in (P2, P19). These training programs were usually carried out online and finished with an evaluation to assess comprehension levels. The main purpose of these initiatives is to maintain employees consistently informed about cybersecurity risks and up to date with the most recent security measures. A minority of participants mentioned the absence of any training opportunities at their workplace, thus expressing a desire to receive such training due to feelings of being uninformed (P16, P18). This is in line with previous research, highlighting the importance of security training or education on security behavior [38].

Training Format. One of the main sentiments among participants was mixed feelings regarding the usefulness of training. The consensus appears to be that training plays a crucial role in education, particularly in fostering employee awareness through transparent communication (P19). This viewpoint is especially emphasized by participants from the cybersecurity sector:

> *"The other issue is, of course, people, and at the end of the day you can only sensitize people with training, awareness campaigns and communication. There is no other option, because you can't prevent human error in any other way than with awareness."* (P13).

Further, many participants highlighted positive experiences with training initiatives, including interactive sessions that were both informative and enjoyable, leaving them with an enhanced sense of security and satisfaction, consequently influencing their subsequent behavior. (P2, P4, P5, P16, P19). Nevertheless, a prevalent criticism among participants pertains to the repetitive nature of training sessions, often characterized by a superficial engagement by just clicking through them. Furthermore, the time-intensive nature of these sessions, coupled with the high workload of primary tasks, was a common source of stress and frustration among participants (P5, P7, P8, P9, P11). This combination of factors often leads to feelings of boredom, dissatisfaction, and alienation, as the training modules were seen as burdensome and overly bureaucratic. Research highlights that security fatigue can result from the method and quantity of security communications and training method [39], [40]. In contrast, other training formats, such as stories as informal lessons or group discussions, can result in better security practices and higher motivation [41], [42]. Research highlights that employees have specific needs regarding security training [43].

D. Detect

Detection of Threats. Most participants reported successfully identifying and preventing cybersecurity threats, particularly phishing attacks, by recognizing deceptive emails and harmful links before any damage occurred. Nearly all participants received simulated phishing emails to assess previous training effectiveness. Many documented cases where employees quickly informed IT or cybersecurity departments about detected threats (P2, P12, P15, P17).

Sense of Achievement in Detection. In contrast to stress, some employees felt a sense of achievement or joy when they successfully detected and defended against threats (P20). Furthermore, in addition to the sense of accomplishment, participants also expressed that this way they managed to avoid additional training, as exemplified by one participant (P2):

> *" ...a sense of achievement. I know it's not an achievement it's a mild sense of, you know, accomplishment a*

very mild sense of that you somehow avoided a training again.".

Overall, the detection of cybersecurity incidents often led to a mix of relief and anxiety among employees. Relief that the threat was identified in time, and anxiety over what could have happened if the breach had succeeded. This emotional duality underscores the personal impact of cybersecurity threats on employees' sense of security and well-being. This extends previous literature that rather showed only positive emotions following the successful identification of phishing [21].

False Alarms or Warnings. Some participants expressed feelings of stress, overwhelm and frustration related to false alarms or the high number of security alerts that they have to deal with. This often leads to alert fatigue, whereby the constant vigilance required can become overwhelming and thus potentially reduce the effectiveness of detecting genuine threats (P15, P17). Previous studies indicate that security notifications can provoke strong emotional reactions [44]. However, users are becoming desensitized to frequent exposure and false alarms, believing they can recognize the risk [45].

E. Respond

Experienced Incidents. Participants described various experiences with cyberincidents (e.g., P1, P6, P10, P14). For instance, a large project was severely disrupted when all operational systems were compromised by an incident (P10). Another example is a critical incident that occurred, where a phishing email caused a complete shutdown of all systems for months, leading to widespread chaos and disruption of patient care (P1). Participants who experienced or were involved in cybersecurity incidents mentioned the emotional consequences they experienced, such as feeling vulnerable, stressed out, helpless, or doubting their own capabilities. An example of this is the following quote (P14):

"...you always feel a bit stupid after something like that, right? So at first I thought OK, yes, I've actually been a victim of a phishing attack, so you question yourself or somehow have self-doubts about yourself and think am I really that easy to deceive...I'm easy to deceive. And, in the same way, self-doubt, I would say, of course you also feel guilty ".

Further participants described instances in which cyberattacks have directly affected operational capabilities and exploited specific systems underscoring the significant functional disruptions that follow (P10, P14). An example is the following statement (P1):

"[I] was then taken away from the entire outside world and all interfaces...it was pure chaos [...] in the end, because we could no longer do our work, the workload simply couldn't be managed at all [...] You have to imagine that you're working with patients, which means it's also very stressful, because after all, it's about human lives and we couldn't communicate important and relevant data to patients. For example, when it comes to what we do next, chemotherapy, how we do it now, how the treatments continue...".

Participants also described the rapid measures their organizations took to isolate the affected systems to prevent further damage. Organizations often rely on pre-established emergency response strategies, which involve implementing communication restrictions and promptly conducting IT investigations to pinpoint the scope and source of the breach. Hence, this often includes taking critical systems offline and cutting connections to internal and external networks to bring the situation under control (P1, P6, P10). Only a limited amount of research explores the consequences of incidents for users in organizational contexts. These studies, however, emphasize the impact of incident experiences on future behaviors and learning [7], [46], [47].

F. Recover

Enhanced Security Measures Post-Incident. Following a breach, organizations typically take advantage of the opportunity to strengthen their cybersecurity defenses. The recovery process involves more than just restoring systems; it also includes enhancing them through significant upgrades to security protocols. Participants highlighted actions such as implementing stricter access controls, enforcing complex password requirements, and enabling multi-factor authentication as common practices. Furthermore, there was an emphasis on enhancing defensive mechanisms by incorporating advanced threat detection technologies and developing improved strategic plans to better protect against future attacks (P10, P13, P19).

G. Organizational Factors

Communication within Organizations. Participants highlighted the importance of structured communication about cybersecurity updates and incidents to internal stakeholders. They explained that this process requires providing consistent information about potential threats and outlining the necessary actions for employees to address those threats (P1, P7, P12, P16). Structured communication protocols were described to be essential for keeping staff informed and prepared for security challenges. Additionally, participants said to value security more when they see their organization prioritizing it (P10). Despite the overall positive communication environment, a significant number of participants pointed out instances of communication gaps where they felt inadequately briefed on specific protocols or updates (P3, P9, P14, P20). These gaps involved unclear communication of IT security roles and procedures, leading to employee frustration, as exemplified by one participant (P20):

"it's often the case that things like this are introduced without sufficient communication beforehand and that's often a problem. Then you find yourself the next day realizing I want to log in, I need my cell phone to do so, but I don't even have it on me now. So, if you communicate this sufficiently in advance, perhaps with

a brief explanation, you can introduce it with a lot of acceptance.".

While version 2.0 of the NIST-CSF introduced more explicit communication-related subcategories compared to version 1.1, which we built our study on (e.g., RS.CO-01, RC.CO-03), these primarily target high-level coordination and incident response. However, our interview data suggest that practical, employee-centered communication, particularly in advance of changes to security procedures, is still insufficiently addressed in practice and remains a source of friction.

Relationship to Experts. Many employees expressed trust in designated security experts within the organization. These experts were seen as reliable sources of support and guidance, often helping employees in navigating security procedures and handling incidents efficiently (P2, P11, P14, P16). Trust was mentioned as essential for effective security oversight and employee security. While generally strong, trust levels varied based on personal experiences and perceptions of the IT department's response to incidents. Some employees expressed disappointment when their expectations of support were not fulfilled, particularly in critical situations where the response was considered insufficient, in some cases leading them to hold the company responsible for the repercussions they faced (P9, P14). Initial findings indicate that this relationship may be dysfunctional, with negative feelings present between users and experts within organizations [32]. Further, [48] displays that the way security advocates deliver security content to users is necessary to overcome negative perceptions towards security.

Enhanced Security Policies for Remote Work. Interestingly, a few participants pointed out that in the transition to remote work, cybersecurity policies within their company have notably intensified (P17); for instance, a heightened focus on safeguarding digital communications and operations. Participants described that they now face stricter security measures on company devices, including disabled audio on laptops and restricted access to approved phone apps. Additionally, the implementation of triple-factor authentication underscores the rigorous security steps taken, involving multiple logins and device checks to ensure a secure network connection (P3).

V. Results: Key points of contact from NIST-CSF

We identified several subcategories within the NIST-CSF that either directly or indirectly referenced points of contact between employees and organizational cybersecurity. Here, selected examples are displayed. For a complete overview of the mapping of the interview results and the subcategories of NIST-CSF, please see Appendix C.

Identify: Awareness of key contacts: The subcategory ID.GV-2 emphasizes clearly defined and coordinated cybersecurity roles, thus, directly shaping employees' understanding of whom to approach for guidance or in case of incidents. RS.CO.1 underlines the importance of employees knowing their roles and operational procedures during incidents.

Protect: Regular Password Changes/ Use of Multifactor Authentication: Additionally, subcategories like PR.AC-1, which is related to identity and credential management, shape frequent points of contact through authentication practices.

Identify: Training Offering/Format: Further, the subcategory PR.AT-1 revolves around training and awareness initiatives, reflecting structured interactions aimed at sensitizing employees to cybersecurity risks.

In addition to the mapped key points of contact, our analysis of the NIST-CSF revealed additional subcategories that represent further potential key points of contact for employees, but for which the interview data provided no direct evidence. For example RS.RP-1 ("Response plan is executed during or after an incident") highlights the moment when employees may need to follow established response procedures. This seems relevant in practice, as employees are often the first to react to incidents and are expected to adhere to predefined steps. Another example is RS.CO-1 ("Personnel know their roles and order of operations when a response is needed"). This code highlights the importance of employees understanding their responsibility and procedures during an incident. This seems to be an important key point of contact, since uncertainty or lack of guidance can result in hesitation or errors when reacting to a cybersecurity incident.

A full table of these additional codes can be found in Appendix D.

VI. Results: Mapping

Based on the results from the interviews and the analysis of the NIST-CSF, we visualize all essential subcategories in Figure 1. To support the interpretation of Figure 1, we provide Table "NIST-CSF Mapping" in Appendix C, which lists all mapped NIST-CSF subcategories alongside their corresponding framework function, full descriptive label, and a representative quote from the employee interviews.

The outer ring of Figure 1 visualizes gaps that emerged across interviews but are not explicitly addressed in the structure of NIST-CSF 1.1. These include, for example, usability challenges, emotional impacts, or missing role clarity in incident response.

At the center of the figure, the Communication Gap and Coping Gap represent fundamental, cross-cutting challenges that permeate all functions and employee interactions with cybersecurity. Rather than being tied to a specific category, they reflect systemic weaknesses in organizational communication and emotional support structures. Further, we formulate the following employee-centric functions:

Identify: The Identify function involves recognizing key cybersecurity roles, responsibilities, and policies. This includes the ability to identify designated contacts and understand the roles responsible for security issues within the organization (ID.GV-1), as well as being aware of relevant cybersecurity policies and how they apply to daily work practices (ID.GV-2).

Protect: This function comprises of two main facets. For the function of "protect", we made a distinction in preventive measurements (e.g. technical controls and security protocols) and the educational process behind activities, aiming to

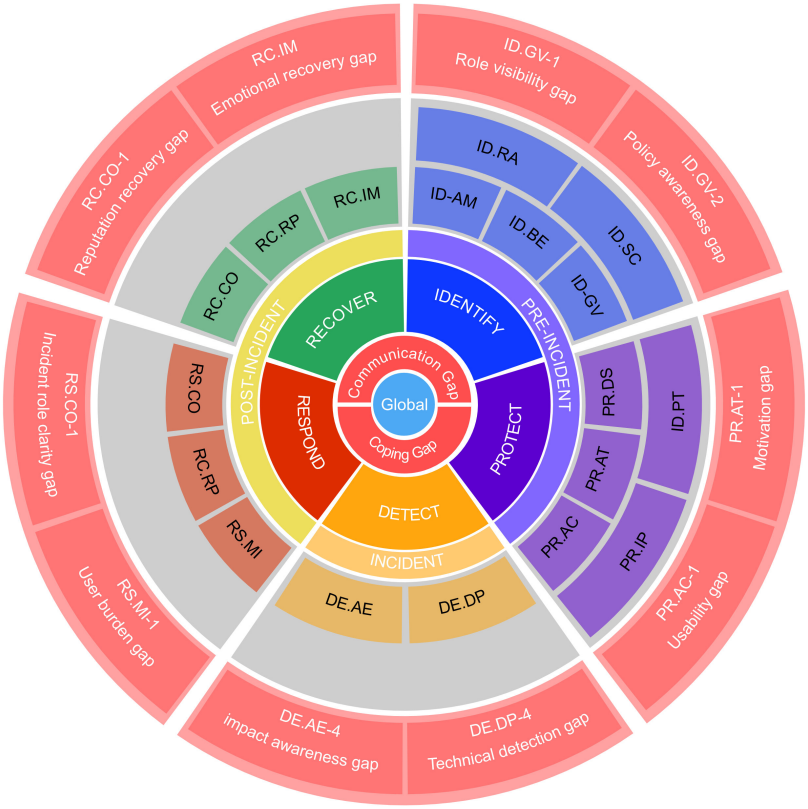


Fig. 1. Employee-centered aspects of NIST-CSF and identified gaps

be well-informed and trained concerning security practices. Firstly, 'protect' involves adherence to security procedures and behaviors, including conformity with policies in a broad sense, or technical frameworks to prevent incidents. This includes technical measures like using secure passwords or encrypting emails containing sensitive information (PR.AC-1). Some employees acknowledged the importance of these measures but expressed frustration with requirements like frequent password changes or complex configurations regarding security technology, which led to workarounds such as writing passwords down. Secondly, prevention entails actively or passively acquiring knowledge on security procedures, such as training sessions or awareness initiatives (PR.AT-1). While these educational efforts were seen as essential, employees often found them repetitive and time consuming, leading to disengagement. Notably, emotional impact of the stated measures (such as regular password changes) and the emerging usability challenges were not addressed by the NIST-CSF.

Detect: This function pertains to the identification of either an event, for instance, an unsuccessful attack, like successfully spotting a phishing email, or on the other hand, an event, which involves a triumphed attack resulting in repercussions for data and systems, such as encountering a successful breach. Thus, 'Detect' refers to the identification of security events. It involves recognizing both unsuccessful attacks, such as spotting and reporting a phishing mail, and successful breaches, where a cyberattack leads to broader consequences on the organization. Employees reported success in identifying phishing attacks and alerting IT personnel (DE.DP-4). However, some also mentioned the challenge to differentiate between real threats and false alarms, leading to alert fatigue and a reduced ability and willingness to respond effectively to new threats.

In addition to technical detection systems, the role of employee awareness is crucial in recognizing and reporting potential incidents. While automated systems detect most threats, employees play a critical part in identifying subtler attacks, such as social engineering. This highlights a gap in the 'detect' function, where the focus is only on technical solutions, while human factors, such as experiences and learning processes with detection processes, are not addressed.

Respond: 'Respond' refers to the immediate reaction to an

incident – often only passively experienced by employees. It ensures effective communication, analysis, and coordination during the event. Employees reported that, in response to incidents, cybersecurity teams quickly isolated affected accounts and systems, effectively containing the damage and preventing further breaches (RS.MI-1). However, some employees expressed frustration over the lack of communication during the incident, which led to confusion and anxiety.

An important aspect of 'respond' is the coordination of communication (RS.CO-1). Employees highlighted that timely and clear updates were essential for reducing uncertainty. Lack of communication left the employees unsure and heightened stress. The respond function in NIST-CSF emphasizes technical containment but does not address the role of communication in maintaining employee confidence and minimizing disruption during incidents.

Recover: 'Recover' focuses on restoring systems, data, and business operations after a cybersecurity incident and resuming normal operations or even modifying the initial condition to improve resilience. This contains the execution of predefined recovery plans, the incorporation of lessons learned into future strategies, and the transparent coordination with either internal and external stakeholders.

Effective recovery means not just returning to the previous state, but adapting and enhancing the organization's resilience against cyber threats. Recovery plans must therefore be well-communicated, regularly tested and adjusted based on real incidents. The NIST-CSF highlights this in subcategories such as RC.RP-1, where recovery procedures are put into practice, RC.IM, which emphasizes improvement through incident review and RC.CO, focusing on stakeholder coordination.

While the 'recover' function provides a robust framework for technical restoration and stakeholder coordination, it does not pay attention to psychological and interpersonal consequences of cybersecurity incidents. Interview findings suggest that the effects of cybersecurity incidents frequently persist after the technical issues have been resolved. Participants reported the feelings of guilt, self-doubt, and even long-term stress or burnout. In several cases team members expressed lacking motivation, considered leaving their jobs due to the overwhelming strain caused by incidents, or described a loss of trust in digital systems. While systems can be restored, trust, moral, and mental well-being may remain fractured. While the technical processes are covered in detail, the recover function offers only very limited guidance for addressing the emotional aspects of post-incident rebuilding.

General: In addition to these core functions, we found the global communication infrastructure between cybersecurity experts and employees throughout all stages to be highly relevant. Effective communication of cybersecurity activities within the organization is crucial for maintaining awareness and ensuring a coordinated response during incidents. This includes the communication of important policies, security procedures, and outcomes from management to operational levels, as well as raising awareness among employees. Many employees reported that they trusted designated cybersecurity experts and saw them as reliable sources of support during incidents. However, a significant number of participants highlighted communication gaps, particularly when new security protocols were introduced without adequate prior notice, leading to confusion and frustration.

In addition, communication of cybersecurity activities is vital not only for operational efficiency but across all functions, e.g., for raising awareness about security responsibilities among employees. Ensuring that cybersecurity roles and policies are effectively communicated across all levels is crucial to maintaining alignment and preparedness within the organization.

The NIST-CSF 2.0 addresses this aspect more prominently than version 1.1 by introducing specific outcomes focused on communication in both the Respond (RS.CO) and Recover (RC.CO) functions. However, the NIST-CSF 2.0 continues to emphasize top-down communication in critical phases, while employee concerns, such as insufficient advance notice or lack of clarity regarding day-to-day procedures, remain underrepresented. This suggests that, despite structural improvements, practical communication challenges persist at the operational level.

VII. Discussion

Research has long recognized the importance of employees in organizational cybersecurity, acknowledging their dual role in both strengthening and potentially compromising security systems [1], [2], [15]. Despite this understanding, promoting secure employee behavior continues to be a challenge, indicating that existing frameworks may inadequately represent the complex dynamics between employees and security measures, underscoring the need for a deeper exploration of the key points of contact that significantly impact employee engagement with security practices. To address this gap, we conducted semi-structured interviews (n=20) to assess an employee's perspective on the key points of contact based on the functions of the NIST-CSF. Additionally, we performed a detailed analysis of the NIST-CSF and identified subcategories where employees may make contact with security. In a final step, we mapped the resulting interview structure to the identified employee-centric subcategories within the NIST-CSF to establish an employee-centric framework of cybersecurity.

While the NIST-CSF provides a comprehensive structure for managing organizational cybersecurity, our analysis reveals notable gaps, both at the framework level and within specific subcategories, when viewed through the lens of employee experience. The framework often remains technology- and process-centric, with very limited attention to the interactions between employees and cybersecurity structures.

The interview data highlights that employees frequently encounter points of contact, such as password changes, mandatory trainings, or multi-factor authentication, in ways that elicit frustration, cognitive overload, or even resistance. Yet, these consequences are not addressed within the NIST-CSF. For example, while subcategories like PR.AC (identity and credential management) and PR.AT (awareness and training)

set requirements for technical implementation and information dissemination, they do not account for usability, motivational barriers, or emotional factors. Employees recurrently described those factors as shaping their day-to-day security behavior.

In addition, the NIST-CSF presumes effective communication of roles, policies, and incident procedures, but offers no reassurance that employees actually understand or internalize these directives (ID.GV-1, ID.GV-2, or RS.CO-1). While employees acknowledged the presence of cybersecurity specialists, awareness of their roles and responsibilities was not always clear, indicating a need for clearer communication of cybersecurity policies and contacts (ID.GV-1, ID.AM-6). Similarly, in the aftermath of incidents, the Recover function covers organizational restoration and reputation management, but does not take the psychological and interpersonal consequences into account that can persist among affected staff (RC.CO-1, RC.IM). Interestingly, participants were only hardly able to differentiate between 'respond' and 'recover'.

Employees reported uncertainty regarding whom to contact during a crisis, emotional fallout from incidents, and a sense of resignation in the face of overwhelming security measures. These recurring issues are conceptualized in our research as employee-centric cybersecurity gaps, such as the Policy Awareness Gap, Usability Gap, or Emotional recovery Gap. This illustrates how employee experiences often conflict with assumptions in the NIST-CSF, specifically that roles are well-defined, policies are adhered to, and communication is effective. Thus, while the NIST-CSF effectively addresses technical and procedural needs, it provides only limited guidance for the complex human factors that ultimately determine the success or failure of security practices. Our approach, using data triangulation, however, offers a new employee perspective on cybersecurity.

A. Recommendations for Practitioners

Approach the employee's role in security holistically. While much research focuses on prevention measures [6], [49], our findings show that focusing narrowly on preventive aspects overlooks the broader set of interactions employees have with cybersecurity on a daily basis. A holistic approach encompasses a breadth of points of contact, from policy identification to emotional recovery from an incident. Practitioners should therefore adopt an employee-centric lens in designing security processes or implementing the NIST-CSF, ensuring that cybersecurity processes are not considered in isolation but in context. For instance, when designing crisis communication, employees' emotional responses to the incident should be considered and addressed to prevent psychological distancing.

Make security support visible and accessible. Several interviewees were unaware of whom to contact in case of a security incident. Although the NIST-CSF requires defined roles (e.g. ID.GV-2), it does not ensure that employees recognize or trust these contacts. Organizations should visibly promote support structures, such as naming contact persons in on-boarding materials, sending periodic reminder emails with IT security contacts, and appointing team-based security contacts who serve as accessible points of contact for security-related issues, which could improve trust and encourage early reporting. Here, focus should be placed on resolving psychological and interpersonal issues with cybersecurity, as pointed out by [6], [50].

Balance protection with usability. Strict controls like frequent complex password changes or multi-step authentication can frustrate employees, causing work delays or risky behavior like writing down passwords. NIST-CSF subcategories such as PR.AC-1 addresses identity management but overlooks usability. Our data suggests that employees respond more positively when security tools are also more convenient (e.g., smartphone-based (2FA)). In line with previous research, we recommend aligning protective measures with actual workflows by testing usability with employees, offering password managers, and ensuring that new security measures support rather than hinder day-to-day tasks [51].

Redesign training to boost engagement. Awareness training is essential, but many participants seem to experience it as boring and irrelevant. While the NIST-CSF demands delivery (e.g., PR.AT-1), they do not address aspects concerning engagement and individualization. Awareness programs should be interactive, role-specific, and frequent, but short. Employees should be invited to reflect on their own role in organizational cybersecurity and contribute feedback. Making training meaningful and integrated into day-to-day work could reduce resistance and help employees internalize good practices.

Acknowledge emotional impacts. In line with previous results, our data shows that security processes (not only active engagement but also passive experience) can trigger stress, guilt and other negative emotions, especially after phishing simulations or real incidents, ultimately resulting in negative behavioral tendencies [7], [21]. The NIST-CSF lacks provisions for psychological strain. Organizations should actively mitigate this by spacing out stressful measures, offering psychological support, and fostering a culture of psychological safety, where asking for help with security issues is normalized and supported.

Encourage employees' self-reflection. While much research agrees on the central role of employees in cybersecurity [1], [2], they themselves are still often not able to completely grasp their role within organizational cybersecurity. By utilizing this study's results for self-reflection, individuals can identify their specific roles in cybersecurity, recognize the aspects they are familiar with or actively engage in, and pinpoint areas where they can improve. For this, users can be presented with their roles within the functions of the NIST-CSF and reflect on their familiarity with these aspects and areas for improvement. While traditionally training and preventive measures are emphasized, our results indicate that it is essential to also highlight foundational elements, such as awareness of policies and knowing key contacts or emotional aspects of cybersecurity.

While this paper only offers a first step towards an employee-centric framework of cybersecurity, the identified points of contact, the mapping of these to the NIST-CSF and

the identification of gaps provide valuable direction for the implementation of the NIST-CSF.

B. Limitations and Future Research

While our study provides valuable insights into key points of contact between employees and cybersecurity, several limitations exist that pave the way for future research. To enrich our first steps towards a framework, incorporating the perspectives of security experts will be crucial, bridging potential gaps between employee experience, theoretical frameworks, and expert insights. Further, the relatively small sample size limits the generalizability of our results. Further research could conduct larger-scale studies to confirm the framework. Although this framework provides a comprehensive approach to key points of contact, there remains a gap in understanding how these points interact and affect cybersecurity behavior. In particular, future research could delve further into the key points of contact by investigating the impact of (lacking) fulfillment on cybersecurity behaviors.

Prior research has shown that contextual factors can influence cybersecurity attitudes and practices, for instance, cultural background shapes how individuals and organizations perceive and prioritize cybersecurity, leading to significant cross-country variation in both awareness and implementation of security measures [52], [53]. While our research included various contextual factors such as varying industries, organizational cultures, duration of work experience, and gender, we only interviewed participants from Germany. As a result, our findings may be influenced by cultural norms and infrastructural conditions; therefore, future research could investigate a more diverse population.

Further, our work builds on the subcategory structure of NIST-CSF version 1.1. While CSF 2.0 introduces notable updates, we argue that CSF 1.1 remains highly relevant in practice. Many organizations are still in the process of transitioning to the new version, as the adoption of frameworks (similar to innovations in general), especially in large and hierarchic, regulated, or resource-constrained environments, tends to lag behind official releases [54], [55]. Further, resources are still being developed to support the implementation of version 2.0 (e.g., quick start guides, translations or metrics), indicating that NIST expects organizations to take time adapting to the new version [56]. With the release of CSF 2.0, most of the subcategories used in our mapping remain conceptually intact, albeit with updated labels or structural reorganizations. For example, RS.AN-1 and RS.AN-2 have been merged into RS.MA-02 to reflect a more integrated incident triage process, while ID.GV-2 and ID.AM-6 have been redistributed across new subcategories in the expanded 'Govern' function. Notably, RS.CO-1 concerning personnel's role clarity in incident Response has been removed as a standalone subcatecory, further emphasizing the relevance of our employee-centric lens (please refer to Appendix E for a full comparison). These developments support rather than challenge the core contribution of our framework, which remains applicable across both NIST-CSF versions. Nonetheless, we recommend that future research should explore the implications of these structural changes to validate and extend our findings within the context of the framework's ongoing development.

While our analysis was conducted with reference to NIST-CSF 1.1, the release of version 2.0 brings structural updates and introduces several new or reframed subcategories. These changes reflect incremental improvements in areas such as role definition, communication, and training. However, a systematic comparison (see Appendix F) indicates that the identified gaps from CSF 1.1 remain largely unaddressed in the new version. In particular, the removal of RS.CO-1, formerly focused on incident role clarity, without a functionally equivalent replacement, highlights a continued blind spot. As such, our findings retain their practical relevance and offer a critical lens on how NIST-CSF should be complemented by an employee-centered perspective.

References

[1] V. Zimmermann and K. Renaud, "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset," *International Journal of Human-Computer Studies*, vol. 131, pp. 169–187, 2019.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[3] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022.

[4] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*, 2019.

[5] C. I. Cybersecurity, "Framework for improving critical infrastructure cybersecurity," *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, vol. 4162018, no. 7, 2018.

[6] A. von Preuschen, V. Zimmermann, and M. C. Schuhmacher, "How do you feel about cybersecurity?–a literature review on emotions in cybersecurity," in *International Symposium on Technikpsychologie (TecPsy) 2023*. Sciendo, 2023, pp. 1–13.

[7] K. Renaud, R. Searle, and M. Dupuis, "Shame in cyber security: effective behavior modification tool or counterproductive foil?" in *Proceedings of the 2021 New Security Paradigms Workshop*, 2021, pp. 70–87.

[8] S. Budimir, J. R. Fontaine, and E. B. Roesch, "Emotional experiences of cybersecurity breach victims," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 612–616, 2021.

[9] M. Barrett, J. Marron, V. Y. Pillitteri, J. Boyens, S. Quinn, G. Witte, and L. Feldman, "Approaches for federal agencies to use the cybersecurity framework," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, Tech. Rep., 2021. [Online]. Available: https://doi.org/10.6028/NIST.IR.8170-upd

[10] Computer Security Resource Center, "Cybersecurity - glossary," https://csrc.nist.gov/glossary/term/cybersecurity.

[11] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Developing cyber-resilient systems: a systems security engineering approach," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, Tech. Rep., 2021. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-160v2r1

[12] M. Hogan and E. Newton, "Supplemental information for the interagency report on strategic u.s. government engagement in international standardization to achieve u.s. objectives for cybersecurity," National Institute of Standards and Technology, Tech. Rep., 2015. [Online]. Available: https://doi.org/10.6028/NIST.IR.8074v2

[13] H. Petrescu, "The future of cybersecurity: Human-centred design," https://research.aurainfosec.io/advisory/the-future-of-cybersecurity-human-centred-design/, 2023.

[14] T. Rahman, R. Rohan, D. Pal, and P. Kanthamanon, "Human factors in cybersecurity: A scoping review," in *Proceedings of the 12th International Conference on Advances in Information Technology*, 2021, pp. 1–11.

[15] B. Schneier, *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.

[16] C. Faklaris, L. Dabbish, and J. I. Hong, "A framework for reasoning about social influences on security and privacy adoption," in *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–13.

[17] I. Security and P. Institute, "Cost of a data breach report 2024," July 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[18] M. Grobler, R. Gaire, and S. Nepal, "User, usage and usability: Redefining human centric cyber security," *Frontiers in big Data*, vol. 4, p. 583723, 2021.

[19] A. Demjaha, S. Parkin, and D. Pym, "The boundedly rational employee: Security economics for behaviour intervention support in organizations," *Journal of Computer Security*, vol. 30, no. 3, pp. 435–464, 2022.

[20] A. Oulasvirta, J. P. P. Jokinen, and A. Howes, "Computational rationality as a theory of interaction," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3491102.3517739

[21] A. Von Preuschen, M. C. Schuhmacher, and V. Zimmermann, "Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity," in *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, 2024, pp. 623–642.

[22] R. Rohan, B. Papasratorn, W. Chutimaskul, J. Hautamäki, S. Funilkul, and D. Pal, "Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the nist cybersecurity framework," in *Proceedings of the 13th International Conference on Advances in Information Technology*, 2023, pp. 1–16.

[23] T. W. Buchanan, "Retrieval of emotional memories." *Psychological bulletin*, vol. 133, no. 5, p. 761, 2007.

[24] E. A. Kensinger, "Remembering the details: Effects of emotion," *Emotion review*, vol. 1, no. 2, pp. 99–113, 2009.

[25] P. Spector, "Job-related affective well-being scale (jaws)," https://paulspector.com/assessments/pauls-no-cost-assessments/job-related-affective-well-being-scale-jaws/, 2019.

[26] P. T. V. Katwyk, S. Fox, P. E. Spector, and E. K. Kelloway, "Using the job-related affective well-being scale (jaws) to investigate affective responses to work stressors," *Journal of Occupational Health Psychology*, vol. 5, no. 2, pp. 219–230, 2000. [Online]. Available: https://doi.org/10.1037/1076-8998.5.2.219

[27] S. R. Kessler, S. Pindek, G. Kleinman, S. A. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health informatics journal*, vol. 26, no. 1, pp. 461–473, 2020.

[28] P. Desmet, "Measuring emotion: Development and application of an instrument to measure emotional responses to products," *Funology 2*, pp. 391–404, 2018.

[29] P. Desmet, P. Wassink, and Y. Du, "Premo (emotion measurement instrument) card set: Male version," Delft, Netherlands, 2019.

[30] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[31] ——, *Thematic Analysis: A Practical Guide*. SAGE Publications Ltd, 2021.

[32] U. Menges, J. Hielscher, A. Buckmann, A. Kluge, M. A. Sasse, and I. Verret, "Why it security needs therapy," in *European Symposium on Research in Computer Security*. Springer, 2021, pp. 335–356.

[33] J. Hielscher, U. Menges, S. Parkin, A. Kluge, and M. A. Sasse, "{"Employees} who {Don't} accept the time security takes are not aware {Enough"}: The {CISO} view of {Human-Centred} security," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2311–2328.

[34] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: a theory-based literature review," *Management Research Review*, vol. 37, no. 12, pp. 1049–1092, 2014.

[35] W. A. Cram and J. D'Arcy, "Barking up the wrong tree? reconsidering policy compliance as a dependent variable within behavioral cybersecurity research," *Information Systems Frontiers*, pp. 1–12, 2025.

[36] S. Ruoti, B. Roberts, and K. Seamons, "Authentication melee: A usability analysis of seven web authentication systems," in *Proceedings of the 24th international conference on world wide web*, 2015, pp. 916–926.

[37] J. Hielscher, M. Schöps, U. Menges, M. Gutfleisch, M. Helbling, and M. A. Sasse, "Lacking the tools and support to fix friction: results from an interview study with security managers," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 131–150.

[38] S. Hu, C. Hsu, and Z. Zhou, "Security education, training, and awareness programs: Literature review," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 752–764, 2022.

[39] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 4, pp. 249–257, 2019.

[40] W. A. Cram, J. G. Proudfoot, and J. D'Arcy, "When enough is enough: Investigating the antecedents and consequences of information security fatigue," *Information Systems Journal*, vol. 31, no. 4, pp. 521–549, 2021.

[41] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012, pp. 1–17.

[42] X. Chen, M. Sacré, G. Lenzini, S. Greiff, V. Distler, and A. Sergeeva, "The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment," in *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024, pp. 1–21.

[43] A. von Preuschen, C. Benda, M. C. Schuhmacher, and V. Zimmermann, "Fear, fun or none: A qualitative quest towards unlocking cybersecurity attitudes," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 2025, pp. 1–24.

[44] C. D. Conrad, J. R. Aziz, J. M. Henneberry, and A. J. Newman, "Do emotions influence safe browsing? toward an electroencephalography marker of affective responses to cybersecurity notifications," *Frontiers in Neuroscience*, vol. 16, p. 922960, 2022.

[45] K. Krol, M. Moroz, and M. A. Sasse, "Don't work. can't work? why it's time to rethink security warnings," in *2012 7th international conference on risks and security of internet and systems (CRiSIS)*. IEEE, 2012, pp. 1–8.

[46] C. M. Patterson, J. R. Nurse, and V. N. Franqueira, "Learning from cyber security incidents: A systematic review and future research agenda," *Computers & Security*, vol. 132, p. 103309, 2023.

[47] P. Mayer, Y. Zou, B. M. Lowens, H. A. Dyer, K. Le, F. Schaub, and A. J. Aviv, "Awareness, intention,(in) action: individuals' reactions to data breaches," *ACM Transactions on Computer-Human Interaction*, vol. 30, no. 5, pp. 1–53, 2023.

[48] J. M. Haney and W. G. Lutters, ""it's {Scary... It's}{Confusing... It's} dull": How cybersecurity advocates overcome negative perceptions of security," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 411–425.

[49] H. Liang, Y. Xue, A. Pinsonneault, and Y. u, "What users do besides problem-focused coping when facing it security threats," *MIS quarterly*, vol. 43, no. 2, pp. 373–A18, 2019.

[50] J. M. Haney and W. G. Lutters, ""it's Scary...It's Confusing...It's dull": How cybersecurity advocates overcome negative perceptions of security," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 411–425. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

[51] M. A. Sasse and I. Flechais, "Usable security: Why do we need it? how do we get it?" O'Reilly, 2005.

[52] S. Creese, W. H. Dutton, and P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Personal and ubiquitous computing*, vol. 25, no. 5, pp. 941–955, 2021.

[53] F. Herbert, C. W. Munyendo, J. Hielscher, S. Becker, and Y. Zou, "Digital security perceptions and practices around the world: A weird versus non-weird comparison," in *Proceedings of the USENIX Security Symposium*, 2025, to appear.

[54] G. Vagnani, C. Gatti, and L. Proietti, "A conceptual framework of the adoption of innovations in organizations: a meta-analytical review of the literature," *Journal of Management and Governance*, vol. 23, no. 4, pp. 1023–1062, 2019.

[55] F. Damanpour and S. Gopalakrishnan, "Theories of organizational structure and innovation adoption: the role of environmental change," *Journal of Engineering and technology management*, vol. 15, no. 1, pp. 1–24, 1998.

[56] National Institute of Standards and Technology, "Cybersecurity framework," https://www.nist.gov/cyberframework, 2024, accessed: 2025-06-27.

VIII. Acknowledgments

We used Grammarly and ChatGPT for language editing.

Appendix A
Participant Demographics

Participant Code	Age	Gender	Industry	Work Experience (in years)
P1	25-29	f	Healthcare	0-1
P2	35-39	m	Computer Science	7-10
P3	25-29	m	Heating Systems	2-3
P4	25-29	f	Private Institute	4-6
P5	25-29	f	Consulting	2-3
P6	50-54	m	Consulting	<21
P7	25-29	f	Marketing	4-6
P8	30-34	f	Bank	4-6
P9	20-24	f	Financial	4-6
P10	25-29	m	Civil Engineering	2-3
P11	30-34	f	Wholesale Banking - Lending	4-6
P12	30-34	f	Investments	2-3
P13	30-34	f	Management consulting	4-6
P14	25-29	f	Investments	0-1
P15	25-29	m	Executive Search	2-3
P16	25-29	f	Internal Audit	4-6
P17	30-34	m	Banking	4-6
P18	25-29	f	Teaching, Research	2-3
P19	50-54	m	Data, Tech & Innovation	<21
P20	50-54	m	IT	<21

TABLE I
PARTICIPANT DEMOGRAPHICS. N=20.FOR PRIVACY REASONS AGE AND WORK-EXPERIENCE IS DISPLAYED IN CATEGORIES.

Scale	Variables	M	SD	Min	Max	Median
ISCI	ISCI_Practices	7.00	3.04	3.00	13.00	6.50
ISCI	ISCI_Importance	12.35	2.54	5.00	15.00	12.50
ISCI	ISCI_Laxness	12.60	2.58	6.00	15.00	13.00
ISCI	ISCI_Score	10.65	1.87	5.67	13.33	10.83
JAWS	JAWS_Total_Score	3.71	0.35	2.85	4.35	3.70

TABLE II
INTERVIEWEE SCREENING: ISCI AND JAWS

Variable	M	SD	Min	Max
IT-Expertise	4.65	0.93	3.00	06.00
CS-Expertise	3.70	1.30	2.00	07.00

TABLE III
IT-AND CS-EXPERTISE

Appendix B
Interview Guide

A. Before the interview:

- consent form in the survey
- Survey with demographic questions and two preparatory questions: What experiences do I have with cybersecurity in my day-to-day work?
- Presentation of the Areas of Cybersecurity in the survey: Identify, Protect, Detect, Respond & Recover
- And the global communication infrastructure between cybersecurity experts and employees during all phases:
  Identify: The first step is to identify what is significant for cybersecurity within the company.
  Protect: This involves procedures and behaviors, adherence to policies in general, or technical structures to prevent incidents, as well as prevention in terms of active or passive approaches to security knowledge.
  Detect: This describes either an attack, that is, an attempted attack that has not yet succeeded, or an incident, meaning a successful attack with consequences for data and systems.
  Respond: This section considers the immediate reaction to an incident.
  Recover: Describes the recovery from an incident and the return to normal operations, or even changes following an incident.
  And the *global infrastructure for communication* between cybersecurity experts and employees during all phases.

B. During the interview:

Introduction

- Participants were welcomed
- Participants were introduced to the interview topic
- Participants were reminded about the sensitive topic and the confidential handling of their data. It was emphasized that the data cannot be traced back to them. They were assured that there was no right or wrong in their answers, and they were encouraged to provide honest and conscientious responses without worrying about what was expected.
- Digital whiteboard Miro was screenshared (to record relevant information)
- It was noted that the interview would be recorded, and they were asked if they had any questions in advance.

Cybersecurity and the associated emotions

- How would you define cybersecurity? or
- What do you associate with cybersecurity in the workplace? (Name three terms that come to your mind)
- Interviewer provided the definition of cybersecurity employed in this study.
- When you think of cybersecurity, how does it make you feel?
- PrEmo was displayed on Miro. Participants were asked to identify their emotional responses towards cybersecurity by selecting the images corresponding to their emotional state from these cartoon characters and asked what those emotions mean to them and to name them.
- The emotion word list was presented, and participants were asked to add any additional emotions.

Experiences and emotions within the cybersecurity areas

- The Areas of Cybersecurity were repeated and displayed on Miro
- Participants were reminded about the two questions in the survey and asked to reflect upon them. They were given the choice to either go through each area or to freely express any experience they specifically remembered.
- Can you describe what experiences you have had with these areas?
- What emotions were felt?

APPENDIX C

NIST-CSF MAPPING

Function from NIST-CSF	Subtheme from Interview	Example	NIST-CSF Subcategory
Identify	**Awareness of Key Contacts**	*"We have a department called ***, which stands for ***, and as far as I know, it's the department responsible for all IT, i.e., cybersecurity issues. Furthermore, this department also serves as the first point of contact." (P5)*	**ID.GV-2** ***(Identify)*** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **Implied NIST Code:** **ID.AM-6** ***(Identify)*** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers, partners) are established
		"We also keep receiving emails, which I find very effective, containing all the contact details. This practice ensures that even those who do not deal with this issue daily are still familiar with the topic and know exactly how to act if they are affected by it." (P11)	**ID.GV-2** ***(Identify)*** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **PR.AT-1** ***(Protect)*** All users are informed and trained **Implied NIST Code:** ***RS.CO-1*** ***(respond)*** Employees know their roles and order of operations when a response is needed. **RS.CO-2** ***(respond)*** Incidents are reported consistently with established criteria **RS.CO-3** ***(respond)*** Information is shared consistently with response plans **Possible gap in framework:**

			NIST-CSF does not reflect informal or ambient awareness-building mechanisms such as repeated low-threshold messaging (e.g., recurring reminder emails). ➔ **Informal reinforcement of security knowledge and psychological readiness are not covered explicitly under existing training or communication controls.**
		"...with the example I gave earlier, about this data security officer, I didn't even know that we had one, nor do I know what exactly his tasks are." (P14)	**ID.GV-2** ***(Identify)*** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **Possible gap in code:** Code does not ensure the visibility or awareness of roles among employees ➔ *Lack of role communication is not addressed* **Implied NIST Code:** **ID.GV-1** ***(Identify)*** Organizational cybersecurity policy is established and communicated
	Policy Awareness	*"I would say we have policies in any case. When a new employee starts, they are given a handbook that explains how to handle IT, what equipment to use, what security measures to take and what policies are in place for this." (P16)*	**ID.GV-1** ***(Identify)*** Organizational cybersecurity policy is established and communicated **PR.AT-1** ***(Protect)*** All users are informed and trained
Protect	**Regular Password Changes**	*"And we were advised to change passwords at regular intervals of 3 to 4 weeks. We were given examples of what passwords should look like: with upper- and lower-case letters, numbers, and special characters. Everyone is responsible for their password and must keep it secret." (P10)*	**PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **PR.AT-1** ***(Protect)*** All users are informed and trained
		"And I remember very well that the internal IT security department was relatively helpless and the only measure they introduced was to increase the length and frequency of the passwords and the frequency with which they had to be changed. So, our iPhones first had a four-digit code, then it became 6 digits and the passwords had to become more complex in order to meet certain requirements. And then I think they had to be changed almost every 8 or 10 weeks, which, when I think of myself now, was a huge source of frustration. Annoyance, because at some point I couldn't remember my passwords anymore. So, I started writing them	**PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **Possible gap in Code:** NIST-CSF does not cover cognitive load, frustration or insecurity authentication may create ➔ *Usability concerns and behavioral consequences are ignored.*

		down, which is actually exactly the opposite effect. I wrote them down somewhere and still forgot the password, which meant that after the third incorrect entry my system was locked and I had to call a hotline to unlock it, but I was 3 minutes before a client call and arrived too late in a call where I was expected. ". (P6)	
	Use of Multi-factor Authentication	*"That's also the issue that with Microsoft Authenticator you now also have the option of using a smartphone or an additional two-factor authentication mechanism to protect yourself better, which is also a bit more convenient." (P15)*	**PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **PR.AC-7** ***(protect)*** Multi-factor authentication is used for network access to privileged and non-privileged accounts **Possible gap in framework:** NIST-CSF does not address how usability or convenience influences user acceptance of security controls. ➔ *User-friendly implementation of security controls is not considered.*
		"And then this constant need to log in with 2 factor authentication is frustrating and hampers workflow. I wouldn't say it's unproductive, but it does lead to dampened work performance." (P10)	**PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **PR.AC-7** ***(protect)*** Multi-factor authentication is used for network access to privileged and non-privileged accounts
	Data Encryption	*"If we now want to go to the second area of protection, i.e. the encryption of files that left the internal e-mail system, for example reports on candidates that were sent to the client, these were forcibly encrypted." (P6)*	**PR.DS-2** ***(Protect)*** Data-in-transit is protected **Possible gap in framework:** NIST-CSF assumes encrypted data-in-transit is effective but does not address usability issues or compatibility challenges at the recipient's side. ➔ Framework does not cover interoperability problems or the emotional consequences (e.g., client frustration, communication breakdown).
	Training Offering	*"And there were online trainings as well, which was where minimum compulsory training, which helped us to know about cybersecurity and how to report the incident or how to detect*	**PR.AT-1** ***(Protect)*** All users are informed and trained

		as well. And what preventive measures we should take…" (P2)	
	Training Format	*"The other issue is, of course, people, and at the end of the day you can only sensitize people with training, awareness campaigns and communication. There is no other option, because you can't prevent human error in any other way than with awareness." (P13)*	**PR.AT-1** ***(Protect)*** All users are informed and trained
		"...at work also involves training courses and things like that, we recently had a situation where you had to click through a training course for an hour and complete it by a certain date, and then you also had to fill out a test to prove that you've looked at it, so to speak, and that perhaps a bit of boredom can be associated with it, because of course it's also time-consuming. You somehow spend an hour of your working time, or maybe even longer, on it. I also have to say that I put it off a bit" (P7)	**PR.AT-1** ***(Protect)*** All users are informed and trained **Possible gap in Framework:** Framework does not consider motivation, emotional resistance or engagement levels → *Trainings are not seen as subjective experiences*
Detect	**Detection of Threats**	*"In my case, it was a phishing email that got through. I recognized it immediately and passed it on to the IT team, communicated with them and they reported back to me that they had blocked it and would check the whole thing again and make sure that nothing more came from this address." (P12)*	**DE.DP-4** ***(Detect)*** Event detection information is communicated Implied NIST Code: **RS.AN-1** ***(Respond)*** Notifications from detection systems are investigated. **Possible gap in code:** RS.AN-1 only refers to notifications from technical detection systems. → *The role of human detection and reporting – which is crucial in real-world settings like phishing – is not reflected in this subcategory, revealing a blind spot in the framework's response analysis process.*
	False Alarms or Warnings	*"Yes, I think at the beginning there was a sense of achievement or a feeling of "we did it". But actually - it's really stressful now, because if it's really a test result from the company, at some point after 3 or 4 attempts you should let it go" (P15)*	**Gap in Framework:** The NIST-CSF does not address the psychological burden or stress caused by frequent cybersecurity testing. → No guidance is provided on optimal test frequency or its emotional impact on employees.
	Sense of Achievement in Detection	*"...a sense of sense of achievement. I know it's not an achievement it's a mild sense of, you know, accomplishment a very mild sense of that you somehow avoided a training again.". (P2)*	**Gap in Framework:** The NIST-CSF does not account for users' emotional responses or behavioral strategies to avoid mandatory training. → NIST-CSF overlooks motivational resistance and the psychological dynamics of cybersecurity compliance.
Respond	**Experienced Incidents**	*"...and in the case of the detection, the hospital was hacked last year, months ago, and as a consequence was removed from the entire outside world and all interfaces internally,*	**RS.MI-1** ***(Respond)*** Incidents are contained

		taken off the network, it probably happened because someone in the hospital clicked on a phishing e-mail. "(P1)	
		"... This then brought the site to a standstill. On a project as big as this, worth 100 million euros, one day of downtime is very costly as everything is related to contractors and infrastructure projects rely on being released and usable by the public. It was a very stressful time as it was initially unclear where the attack was coming from." (P10)	**Gap in Framework:** Describes business impacts and stress during a cyberattack, but not a specific NIST CSF process. → Effects like downtime and uncertainty fall outside the framework's process-focused scope.
		"...you always feel a bit stupid after something like that, right? So at first I thought OK, yes, I've actually been a victim of a phishing attack, so you question yourself or somehow have self-doubts about yourself and think am I really that easy to deceive...I'm easy to deceive. And, in the same way, self-doubt, I would say, of course you also feel guilty" (P14)	**Gap in Framework:** Describes emotional effects after a phishing attack. → The NIST-CSF does not cover personal feelings—no core function addresses such human factors.
		"And if you want to put it in context here, you could even say that by changing this company from an employee-driven company to a technology-driven company like a retailer then online retailer, the focus on IT and thus on cybe security has also become greater and greater and not only rules have been introduced, but also actual ones. Technical security measures to prevent intrusion. But in this very specific case also to prevent the outflow of data" (P6)	**RS.MI-1** ***(Respond)*** Incidents are contained **PR.DS-5** ***(Protect)*** Protections against Dataleaks are implemented
Recover	**Enhanced Security Measures Post-Incident**	*"The 2-factor authentication was also strengthened. If we were inactive for a quarter of an hour, we were automatically logged out and had to log in again. It may be annoying, but it increases security" (P10)*	**RS.IM-1** ***(Respond)*** Response plans incorporate lessons learned **PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **Possible gap in Framework**: does not account for user burden. Only focuses on technical improvement
Organizational Factors	**Communication within Organizations**	*"...it's often the case that things like this are introduced without sufficient communication beforehand and that's often a problem. Then you find yourself the next day realizing I want to log in, I need my cell phone to do so, but I don't even have it on me now. So, if you communicate this sufficiently in advance, perhaps with a brief explanation, you can introduce it with a lot of acceptance." (P20)*	**ID.GV-1** ***(Identify)*** Organizational cybersecurity policy is established and communicated **Possible gap in code:** ID.GV-1 includes the communication of cybersecurity policy but does not address timing**,** clarity**, or** user-centered implementation**.** → The importance of timely, understandable communication as part of change management is not emphasized.

	Relationship to Experts	*"On the other hand, I also have a good feeling about my company. I would say that I feel more protected because we have a very good IT system or very good IT colleagues." (P11)*	**Gap in Framework:** Expresses personal trust in the company's IT team. Interpersonal dynamics are not captured in the NIST-CSF.
	Enhanced Security Policies for Remote Work	*"And then there's the fact that working from home has become even stricter, our company laptops, for example, can't emit any sound or anything else. So you can't hear anything, it's all protected. Our company cell phones can only use special apps that have been approved by the company in advance. So it's all very, very strict. Sometimes it's also a bit restrictive. You can't use certain things to their full extent, simply because of the device. The home office issue has made the whole thing even stricter. This means that we even have 3-factor identification at home. Another login before the real login, then again with a different device. So that's a bit exhausting, but of course it's also clearly understandable." (P17)*	**PR.AC-1** ***(Protect)*** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes **PR.PT-3** ***(Protect)*** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **Possible Gap in Code:** NIST-CSF does not account for the emotional and functional friction experienced by users → *Framework neglects how users perceive restrictions.*

TABLE I
MAPPING OF EMPLOYEES' PERSPECTIVES TO THE EMPLOYEE ASPECTS OF THE NIST-CSF

APPENDIX D

NIST-CSF MAPPING: CATEGORIES THAT WERE NOT MENTIONED IN THE INTERVIEWS

NIST-CSF Function	NIST CSF Subcategory	Rationale
Identify	**ID.RA-1** *Asset vulnerabilities are identified and documented*	Employees can be involved in reporting vulnerabilities (e.g., phishing attempts, misconfigurations, or weaknesses in workflows). Awareness campaigns or vulnerability reporting mechanisms are touchpoints.
	ID.RA-3 *Threats, both internal and external, are identified and documented*	Employees may report suspicious incidents, social engineering attempts, or unusual activity, and may also receive information about threats through training, awareness campaigns, or notifications in case of attacks.
	ID.RA-6 *Risk responses are identified and prioritized*	Risk mitigation measures directly impact employees (e.g., new policies, workflow changes, added security controls). The touchpoint is in the implementation and communication of these risk responses.
Protect	**PR.AC-2** *Physical access to assets is managed and protected*	Employees regularly experience this when using badges, keys, or access controls to enter buildings, rooms, or server areas. It's a daily security contact for many.
	PR.AC-4 *Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties*	Employees may request access to systems or data, or experience denied access. While they do not directly manage permissions, their requests, escalations, or frustrations are key touchpoints (e.g., waiting for access or hitting privilege limits).
	PR.AC-6 *Identities are proven and bound to credentials and asserted in interactions*	Employees must often verify their identity (e.g., showing ID for badge pickup, answering security questions), especially during onboarding or credential reset.
	PR.DS-1 *Data-at-rest is protected*	Employees may interact with data encryption tools or policies (e.g., file encryption, restricted access to sensitive files). For most, the touchpoint occurs via enforced rules or training on how to store data.
		If feedback about security tool performance is collected from employees, this can be a direct touchpoint. Communication about improvements may also reach employees.

	PR.IP-8 *The effectiveness of protection technologies is shared*	
	PR.IP-9 *Response plans (Incident Response and Business Continuity) and recovery plans are in place and managed*	This is a touchpoint for employees who must know and follow these plans (e.g., in a crisis). The touchpoint occurs in training, information material, drills, or real incidents.
	PR.IP-11 *Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)*	Employees directly experience these practices through onboarding, background checks, or exit procedures. This is a classic employee touchpoint, especially when access is removed or provisioned.
	PR.PT-2 *Removable media is protected, and its use is restricted according to policy*	Employees must comply with restrictions on USB drives and other removable media. They may experience prompts, blocked access, or need to request permission.
Detect	**DE.CM-4** *Malicious code is detected*	While technical in nature, it may become a touchpoint if the system is infected (e.g., being notified, asked to take action, or participate in incident resolution).
	DE.DP-1 *Roles and responsibilities for detection are well defined to ensure accountability*	If detection roles include employees (e.g., incident reporting, initial detection duties), this creates a direct touchpoint through assigned responsibilities and communication.
	DE.DP-4 *Event detection information is communicated*	If detection results are shared with employees (e.g., warnings, security advisories, incident notifications), this forms a clear point of contact. Communication of findings may require employee action or awareness.
Respond	**RS.AN-5** *Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources*	Employees may directly report vulnerabilities (e.g., through a reporting system), making this a touchpoint if employee channels are established. External researchers are also a touchpoint (though not “employee” in your sense).
	RS.IM-1 *Response plans incorporate lessons learned*	Employees involved in incident response may participate in after-action reviews, share feedback, or report what did and did not work. Even non-IT staff can be asked for input if the incident impacted them, making this a touchpoint.

	RS.MI-2 *Incidents are mitigated*	Employees can play a role by following new instructions (e.g., updating passwords, applying patches, following new procedures) as part of mitigation. While IT leads the process, end-user participation is usually required to fully mitigate threats.
	RS.RP-1 *The response plan is executed during or after an incident*	Employees are often expected to follow specific steps in the organization's incident response plan. This may include reporting incidents, following communication protocols, cooperating with IT or security teams, and sometimes participating in containment or recovery measures. Their actions are crucial to the effectiveness of the response plan, making this a direct touchpoint between employees and cybersecurity processes.
Recover	**RC.CO-3** *Recovery activities are communicated to internal and external stakeholders, as well as executive and management teams*	Communication to employees about recovery steps is essential for coordinated action and confidence rebuilding. Employees are direct recipients of these communications and may also need to relay information to external stakeholders or adapt their actions based on recovery instructions.
	RC.IM-1 *Recovery plans incorporate lessons learned*	Employees are often the source of critical feedback after an incident. Post-incident reviews (“lessons learned”) typically solicit input from affected staff, not just technical or management teams. Employees may attend debriefs, submit feedback, or help identify what went wrong and what should change, which makes this a touchpoint.
	RC.RP-1 *The recovery plan is executed during or after a cybersecurity incident*	The execution of a recovery plan often involves direct employee engagement, not just IT or management. For example, employees may be required to follow specific procedures, restore data, return to modified workflows, or communicate with key contacts as systems are brought back online. In many organizations, the effectiveness of recovery hinges on employees following instructions, reporting issues, or resuming business processes in accordance with new protocols.

TABLE II
RELEVANT SUBCATEGORIES FROM NIST-CSF THAT WERE NOT MENTIONED IN THE INTERVIEWS

APPENDIX E

NIST-CSF COMPARISON VERSION 1.1 AND 2.0

NIST CSF 1.1	NIST CSF 2.0
ID.GV-1: Organizational cybersecurity policy is established and communicated	**Moved (renamed):** Moved to Govern function. Now part of **GV.PO-01** (Policies, Processes, and Procedures category), which states that cybersecurity policy is established, communicated, and enforced **ID.GV was moved to the Govern function and expanded.**
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**Moved/merged**: In CSF 2.0 this outcome is addressed under the new Govern function. Internal role responsibilities are covered by **GV.RR-02** (Roles, Responsibilities, and Authorities) and coordination with external partners are covered by **GV.SC-02** (Cyber Supply Chain Risk Management). **ID.GV-2 was reworded and split across two subcategories.**
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	**Moved/merged**: Now handled in the Govern function. Workforce roles are encompassed in **GV.RR-02**, and third-party (supplier, partner, customer) roles are in **GV.SC-02** **ID.AM-6 was reworded and split across two subcategories.**
DE.DP-4: Event detection information is communicated	**Moved (renamed): DE.DP-4 was i**ncorporated into the Detect function's analysis outcomes. In CSF 2.0 this appears as **DE.AE-05** (within Adverse Event Analysis), e.g., "information on adverse events is provided to cybersecurity and incident response tools/staff". **DE.DP-4 was reworded and relocated to the Detect category**
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	**Renamed/revised:** Restructured under **PR.AA** (Identity Management & Access Control). Largely corresponds to **PR.AA-01** in CSF 2.0 (organization manages identities and credentials for authorized users, devices, etc.). Some aspects (e.g., auditing) are covered by **PR.AA-06** . **PR.AC-1 was renamed and updated.**
PR.AC-7: Multi-factor authentication is used for network access to privileged and non-privileged accounts	**Merged:** Explicit MFA requirement is not a standalone subcategory in CSF 2.0. It is merged into the broader authentication requirements under **PR.AA-03** (which covers authentication for users, processes, devices). The original **PR.AC-7** identifier has been removed. The content was merged with **PR.AA-03**.
PR.AT-1: All users are informed and trained	**Retained (renamed/reworded):** Becomes **PR.AT-01** in CSF 2.0, with expanded wording (personnel are provided awareness and training to perform tasks securely). **Note:** It also subsumes the concept from **RS.CO-1** (ensuring personnel know their roles in incident response) **PR.AT-1 was reworded.**

PR.DS-2: Data-in-transit is protected	**Retained (reworded):** Still present as **PR.DS-02** in CSF 2.0, with the same outcome (protection of data in transit, now explicitly referencing confidentiality, integrity, availability) **PR.DS-2 was reworded.**
RS.AN-1: Notifications from detection systems are investigated	**Moved/merged:** Shifted to the new **RS.MA** (Incident Management) category. Its function is covered by **RS.MA-02** ("incident reports are triaged and validated"), which consolidates the initial analysis of incidents **RS.AN-1 was merged with RS.AN-2 into RS.MA-02**
RS.CO-1: Personnel know their roles and order of operations when a response is needed	**Merged/removed:** No longer a standalone subcategory in CSF 2.0. Its intent is incorporated into training/awareness outcomes (PR.AT-01) and governance of roles. **The original RS.CO-1 identifier is not used in 2.0**
RS.CO-2: Incidents are reported consistently with established criteria	**Retained (reworded):** Still in the Respond function under **RS.CO-02**. Rephrased as notifying internal and external stakeholders of incidents as required by law, policy, etc. **RS.CO-2 was reworded.**
RS.CO-3: Information is shared consistently with the response plan	**Retained (reworded):** Remains in Respond function as **RS.CO-03**, now explicitly "Information is shared with designated internal and external stakeholders as required by laws, regulations, or policies". **RS.CO-3 was reworded.**
RS.IM-1: Incidents are contained	**Retained unchanged**: Remains as **RS.MI-01** in CSF 2.0 with the same outcome (containment of incidents)

TABLE III

RELEVANT CHANGES IN NIST 2.0 FRAMEWORK

APPENDIX F

COMPARSION OF EMPLOYEE-CENTRIC GAPS AGAINST NIST CSF 2.0 SUBCATEGORIES

Gap	Critical Status	CSF 2.0 Reference	Analysis
Role Visibility Gap (ID.GV-1)	Partially improved but unresolved	**GV.PO-01** *Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities, and is communicated and enforced*	CSF 2.0's Policy outcome (**GV.PO-01**) requires that an organizational cybersecurity policy be established and enforced based on context. This aligns with **ID.GV-1**'s intent is to set policy, but the framework does not ensure that employees actually understand the policy or see how it applies to their own roles. In practice, staff may still be unaware of where their responsibilities fit within the policy framework.
Role Clarity Gap (ID.GV-2)	Partially improved but still incomplete	**GV.RR-02:** *Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced*	NIST requires roles and authorities to be "established, communicated, understood, and enforced" (GV.RR-02). However, this formal structure overlooks whether employees actually grasp related policies. In effect, accountability exists on paper, but real staff awareness of policy details may still be under-addressed.
Motivation Gap (PR.AT-1)	Largely unchanged (training-only focus)	**PR.AT-01:** *Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind*	CSF 2.0 maintains PR.AT-01: Personnel receive awareness training. But motivation is not explicitly targeted.
Usability Gap (PR.AC-1)	Unaddressed	**PR.AA-01:** *Identities and credentials for authorized users, services, and hardware are managed by the organization*	Identity/authentication is emphasized under PR.AA-01 (identities and credentials are managed). No mention is made of usability. The framework ignores whether access controls are user-friendly.
Technical Detection Gap (DE.DP-4)	Partially addressed	**DE.AE-06:** *Information on adverse events is provided to authorized staff and tools*	CSF 2.0 moves the core of DE.DP-4 into DE.AE-06, ensuring information on events is provided to staff/tools. This helps technical response, but employees have no direct role in spotting attacks.
Impact Awareness Gap (DE.AE-4)	Unaddressed	**DE.AE-04:** *The estimated impact and scope of adverse events are understood*	The core still includes DE.AE-04 ("impact and scope of adverse events are understood"). However, this is framed as a systems outcome, not tied to any practical employee action. Staff still are not actively informed of actual event impacts in a meaningful way.
User Burden Gap (RS.MI-1)	Unaddressed	**RS.MI-01:** *Incidents are contained*	CSF 2.0's RS.MI-01 only states that "incidents are contained". It offers no guidance on reducing work disruption or automating tasks for users. The user experience of incident response remains an afterthought, so the burden on employees stays high.

Incident Role Clarity Gap (RS.CO-1)	Unaddressed	Partially transferred to **PR.AT-01:** *Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind*	CSF 2.0 removed the explicit RS.CO-01 requirement (shifted to training). Now there's no outcome clarifying employee incident roles. Workers are left with the same vague role definitions during incidents, so this gap has not improved.
Reputation Recovery Gap (RC.CO-1)	Unaddressed	**None**	NIST's draft dropped RC.CO-01 ("Public relations are managed"). The final CSF only includes broad recovery communications (RC.CO-03/RC.CO-04), with no mention of reputation. Thus, guidance on post-incident reputation Recovery is entirely absent.
Emotional Recovery Gap (RC.IM)	Unaddressed	**None**	The concept of emotional recovery is not in CSF 2.0. The prior RC.IM category was removed, and nothing replaced it. The framework does not address employee stress or morale.
Communication Gap	Unaddressed	**None**	CSF 2.0 still only formalizes incident communications (RS.CO).
Coping Gap	Unaddressed	**None**	There is no element covering employee coping or well-being. The framework emphasizes technical recovery (Recover categories RC.RP, RC.CO) and is silent on mental health.

Employee-Centric Cybersecurity Gaps vs. NIST CSF 2.0 (Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)

TABLE IV

EMPLOYEE-RELEVANT SUBCATEGORIES IN NIST CSF 2.0

Function	Subcategory (CSF 2.0)	Classification	Rationale
Govern (GV) - Organizational Context (CO)	**GV.OC-02**: *Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered*	New	Addresses stakeholder understanding. Employees are key internal stakeholders; this encourages identifying and considering their cybersecurity needs and expectations, improving communication and buy-in across the organization.
Govern (GV) - Risk Management Strategy (RM)	**GV.RM-05:** *Lines of communication across the organization are established for cybersecurity risks,including risks from suppliers and other third parties*	New	Emphasizes communication channels for cybersecurity. For employees, this ensures clear two-way communication on security risks throughout the organization, increasing awareness and collaboration among staff and teams.
Govern (GV) - Roles Responsibilities, and Authorities (RR)	**GV.RR-01:** *Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving*	New	Focuses on leadership and culture. Signals to employees that senior leaders prioritize cybersecurity and ethical behavior, helping to foster a risk-aware culture. This top-down commitment can motivate employees and shape a positive security mindset.
Govern (GV) - Roles Responsibilities, and Authorities (RR)	**GV.RR-02:** *Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced*	Reframed	Clarifies cybersecurity roles and accountability. This clarity can help employees understand their individual responsibilities and promote accountability.
Govern (GV) - Roles Responsibilities, and Authorities (RR)	**GV.RR-03**: *Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities and policies*	New	Ties resources to roles and policies. For employees, this means necessary support (e.g., time, tools, training budgets) is provided to carry out security tasks. Aligning resources with roles helps staff effectively fulfill their security responsibilities.
Govern (GV) - Roles Responsibilities, and Authorities (RR)	**GV.RR-04:** *Cybersecurity is included in human resources practices*	New	Integrates security into HR processes (hiring, onboarding, reviews). Directly employee-centric: ensures that hiring, training, and performance management include security criteria. This embeds security in workforce management and aligns employee development with cybersecurity goals.
Govern (GV) - Policy (PO)	**GV.PO-01:** *Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced*	Reframed	Focuses on creating and communicating security policy. Relevant to employees: it ensures that organizational security policies (rules/expectations) are clearly communicated and enforced. This improves employee awareness of cybersecurity policy and what is expected of them.
Govern (GV) - Supply Chain Risk Management (SC)	**GV.SC-02:** *Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally*	New	Defines roles involving external Parties. It emphasizes coordinated communication across organizational boundaries, so internal staff could understand their responsibilities with external stakeholders.

Protect (PR) - Awareness and Training (AT)	**PR.AT-01:** *Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind*	Reframed (formerly **PR.AT-1**)	Ensures broad security training for all employees. Directly employee-focused: every staff member receives awareness training that equips them to handle everyday tasks securely.
Protect (PR) - Awareness and Training (AT)	**PR.AT-02:** *Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind*	Reframed (formerly **PR.AT-2**)	Targets training for specific roles. Employees in specialized positions (e.g., system admins, SOC analysts) receive tailored training, strengthening their skills for role-specific security tasks.
Respond (RS) - Incident Response Reporting & Communication	**RS.CO-02:** *Internal and external stakeholders are notified of incidents*	Reframed (formerly **RS.CO-2**)	Mandates notifying stakeholders of incidents. From an employee perspective, this means staff (internal stakeholders) are promptly informed of security incidents that affect them.
Respond (RS) - Incident Response Reporting & Communication (CO)	**RS.CO-03:** *Information is shared with designated internal and external stakeholders*	Reframed (formerly **RS.CO-3**)	Ensures the sharing of incident information. Relevant to employees: designated internal stakeholders (teams, management) receive necessary information during incidents.
Recover (RC) - Incident Recovery Communication (CO)	**RC.CO-03:** *Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders*	Reframed	Covers communication of recovery progress. From the employee viewpoint: teams and staff are kept up-to-date on restoration efforts.
Recover (RC) - Incident Recovery Communication (CO)	**RC.CO-04:** *Public updates on the incident recovery are shared using approved methods and messaging*	New	Focuses on public recovery updates. While aimed at external audiences, it promotes a culture of transparency. For employees, this means consistent, approved messaging is used (internally and externally).
Identify (ID) - Improvement (IM)	**ID.IM-04:** *Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved*	Reframed	Covers communication of response and security plans. Critically, it explicitly includes “communicated”. For employees, this ensures that incident response and other security plans are made known and updated, so staff can use and improve them.

TABLE V

NEW AND REFRAMED EMPLOYEE-RELEVANT SUBCATEGORIES IN NISCT CSF 2.0

Chapter 7

Discussion and Reflection

Contents

7.1 Summary of Findings

7.1.1 Goal 1: Identify the emotions and attitudes related to organizational cybersecurity

Prior research on emotions in cybersecurity has largely focused on negative feelings, often unclear in definitions, with few studies exploring the broader spectrum of emotions [165] or employing the tripartite model of attitudes but instead focusing on related constructs [39, 52, 121]. Preliminary findings suggest that understanding emotions and attitudes holistically is crucial for promoting positive behaviors in organizations (e.g., [30, 39, 81]). Thus, we explore the emotions employees have towards cybersecurity (RQ1a) and examine their attitudes using tripartite models of attitudes (RQ1b). Paper A and Paper C identified complex and multifaceted emotional and attitudinal responses towards cybersecurity that extend far beyond simple positive or negative reactions. Further, within Paper B, we explored associations of humans with cybersecurity, revealing both emotions and attitudes towards cybersecurity.

RQ1a. Regarding emotions, in Paper A, we utilized the circumplex model of affect to categorize emotions along two dimensions: valence (negative to positive) and arousal (low to high). The research revealed that employees experience a broad variety of emotions towards cybersecurity, with negative emotions significantly outnumbering positive ones. This tendency towards negative emotions aligns with previous research [164]. Whereas this aligns with prior research, humans also have a greater ability to ability to differentiate negative emotions compared to positive ones [17]. Notably, we identified more low-arousal emotions (such as annoyance, discomfort, or happiness) compared to high-arousal emotions (like insecurity, tension, or fascination), which has not been reported in prior literature. A further new finding was that almost all participants experienced mixed emotions simultaneously. While prior research investigated specific single emotions or general affect in terms of valence (e.g., [30, 101]), our research shows that employees often held contradictory feelings, such as being interested in learning more while feeling intimidated by the complexity of cybersecurity.

RQ1b. Concerning employees' attitudes towards cybersecurity, we found three distinct components in line with tripartite attitude theories [4,175]: affective, cognitive, and conative.

For the affective component, participants described emotions varying in their valence (negative to positive) and arousal (low to high). While some described specific emotions, others expressed general affective tendencies. For specific emotions, many expressed a mix of emotions ranging from annoyance to fear towards security. In Paper A, we found more differentiated emotions as compared to the affective component in Paper C, in which we found vague descriptions and affective tendencies - this, however, is not surprising due to the measurement (Paper A with various emotion measurement tools compared to Paper C not specifically asking for emotions) approach and conceptualization of both terms (see Section

2.3.1, Delimitation of Related Concepts).

The cognitive component revealed that participants viewed cybersecurity through multiple lenses: nearly a quarter described it as a "black box" or unknown entity, over a third associated it with dark or criminal imagery similar to previous research [36], while roughly a third saw it as a protective system. Despite these varied and often negative perceptions, the vast majority, acknowledged cybersecurity's importance, as in previous research [136]. Our results expand upon previous research on mental models, for instance, by illustrating cognitive evaluations and affective associations within narratives [61, 93, 173].

Conatively, participants demonstrated a spectrum of responses ranging from supportive engagement to complete avoidance, with procrastination and minimal effort being common patterns. These results extend previous ones, displaying a broad variety of complex behavioral tendencies [21]. For instance, we uncovered that the theme "awareness and caution", which is primarily associated with positive behaviors in prior literature [121, 122], may potentially be connected to unfavorable behavioral tendencies.

We further identified an interplay between the three components or a prevalence of attitudinal ambivalence, with many participants experiencing conflicts. For instance, recognizing cybersecurity's importance (cognitive component) while simultaneously harboring negative feelings (affective component) about it. Further, we showed that some participants are aware of this ambivalence or discrepancies in knowledge and behavior.

While Paper B looked into S&P associations, some results reflected emotions and attitudes. For instance, in line with Paper C, almost all participants viewed security as important. There was also a tendency towards negative emotions - in particular, worry and fear; some described security as boring or uninteresting.

7.1.2 Goal 2: Understand the factors that contribute to emotions and attitudes in organizational cybersecurity

Research on the causes of emotions related to cybersecurity has explored various influences, including the impact of incidents and how fear appeals can promote better password choices [12, 43, 70]. However, there remains a significant gap in understanding the factors that contribute to emotions and attitudes within organizational cybersecurity. Consequently, our research explored the causes of emotions related to cybersecurity (RQ2a) and the factors that influence employees' attitudes towards this topic, acknowledging its social nature (RQ2b) within Paper A and Paper C.

RQ2a. We identified four essential causes of cybersecurity related emotions, with two of them closely interconnected:

1. Individual factors - personal perceptions:

   Personal perceptions regarding individual factors largely involve prior knowledge and experience, the perceived level of protection, and the degree of autonomy, including feelings of being pressured by cybersecurity requirements.

2. Individual factors - cybersecurity perceptions:

   Cybersecurity perceptions differ from personal perceptions, emphasizing their associations with the concept itself, such as the perceived narrative, relevance, and complexity.

3. Interpersonal factors:

   Interpersonal factors focus on social dynamics between actors within an organization, for instance, self-perceptions and perceptions of others, the level of exchange, or the perceived relationship with experts, such as the lack of proactive communication between both parties.

4. Organizational factors:

   Organizational factors are shaped by factors like the perceived security and error culture, or the perception of design and frequency of education.

While there is prior research on evoked emotions (e.g., [43,70,86]), only one study explores the causes of emotions in cybersecurity inductively [136]. Our research confirms the patterns identified in previous literature, such as lack of knowledge or complexity, and extends them by uncovering a broader variety of themes and a distinct structure.

RQ2b. We found two major areas influencing cybersecurity attitudes: (social) experiences and individual factors.

(Social) Experiences vary along a temporal dimension (past, ongoing, future) and personal distance (direct experiences made by the individual, indirect experiences made by colleagues, peers, or others). We extend prior research that displays the effect of experience on awareness [23] and peer experiences on attitude/behavior changes [130] by a broader variety of (social) experiences. Direct past experiences, for instance, encompass experiences from onboarding or past incident experiences. Indirect ongoing experiences can encompass perceptions of colleagues' behaviors and attitudes, such as perceiving cybersecurity as a topic colleagues do not want to talk about or perceptions of security as time-constraining, as previously displayed in literature [35]. Individual factors focus on various aspects, such as the level of perceived vulnerability or the perceived level of data sensitivity.

In line with Papers A and C, security associations in Paper B demonstrate that cybersecurity is frequently associated with knowledge and experience gaps. Emotions and attitudes exhibit similar themes as causes, which is not surprising given that these two concepts are closely intertwined. However, in line with the conceptualization of attitudes, we observed a greater stability regarding their temporal aspects. Attitudes place a stronger emphasis on time-related factors, such as past experiences and future expectations. Additionally, attitudes tend to be more influenced by social factors. While interpersonal and organizational influences are also present for emotions, social dynamics are particularly relevant for attitudes, especially in terms of vicarious experiences.

7.1.3 Goal 3: Investigate factors to improve cybersecurity-related emotions and attitudes

There is limited knowledge regarding the factors that enhance emotional and attitudinal aspects influencing user engagement. To improve cybersecurity behavior, it is essential to examine the broader consequences of security-related emotions, identify which emotions promote positive behaviors, and develop strategies that encourage these positive attitudes. Thus, we explored the consequences of emotions in cybersecurity (RQ3a) and then investigated factors to make cybersecurity more enjoyable, a positive high-arousal emotion (RQ3b). Subsequently, we explored needs for positive cybersecurity attitudes (and, ultimately, positive cybersecurity behavior; RQ3c).

RQ3a. We revealed a variety of consequences of emotions beyond protective behaviors, including cognitive effects, such as psychological distancing and repression. Psychological distancing refers to a disconnection that occurs when individuals either deactivate their emotions, as previously observed by Burns et al. [30]. Other consequences include externalization, where individuals transfer responsibility from themselves to management or other third parties, as well as positive outcome expectations. Behavioral consequences involve attention levels, awareness, caution, and the effectiveness of the approach taken to learning. Emotions related to security can further lead to social effects, such as seeking social support as previously observed by Liang et al. [101]. Additionally, we identified spill-over effects that extend beyond security-related issues, affecting individuals' personal lives, including emotional exhaustion and reduced productivity.

Our dependency analysis then identified paths alongside the causes-emotions-consequences relationship. We identified distinct pathways for the emotions we examined. When looking at the broader picture, we found that, consistent with the circumplex model of affect, low-arousal emotions generally lead to unfavorable outcomes, while high-arousal emotions are associated with favorable outcomes. However, "interest" is an exception, as it can lead to both positive and negative results (see Paper A for possible explanations). In contrast to previous research that emphasizes fear appeals as a method for promoting positive cybersecurity behavior, our findings indicate that it is not the emotional valence (positive or negative) that matters, but rather the arousal level of the emotions that influences cognitive, behavioral, and social outcomes. While both negative and positive high-arousal emotions can lead to positive outcomes, we recommend adopting an ethical approach by focusing on positive high-arousal emotions.

RQ3b. Consequently, we explore factors for making cybersecurity more enjoyable (high-arousal, positive emotion). In Paper B, we identified several factors that influence the perception of cybersecurity as enjoyable. For example, some participants emphasized that simplification is essential for enjoyment, while others pointed out that a lack of knowledge contributes to the view that security was not fun. Additionally, negative emotions, such as feeling constrained by security communication, are perceived as barriers to enjoyment.

Our findings emphasize the strong relationship between positive perceptions and social aspects, as discussed in Papers A and C. We stress the importance of trust-building between employees and various stakeholders, incentivization, and engaging conversations. In contrast, the popular approach of gamification, often employed through gamified cybersecurity training in organizations, was mentioned only occasionally and was linked to mixed perceptions. Some participants noted that security is a topic that either cannot be or should not be enjoyable.

RQ3c. For attitudes, we identified four central themes that describe the employees' needs for positive cybersecurity attitudes (and positive cybersecurity behavior) from both individual perspectives and collective discussions: (1) social and cultural framework, (2) communication style, (3) education contents, (4) educational formats. In line with prior research, we show that participants strive for simplicity and usability [37,38,144] and extend prior results on personal and individualized learning content such as stories or peer learning [124,129].

Extending the results in Paper B of emotions for attitudes, gamification as part of the types of learning formats, is not only viewed with mixed perceptions, but rather described as suitable only for selected areas of cybersecurity. Participants further formulate the need that the emotional tone of communications and learning material needs to be adjusted to the respective phase. In general, most participants highlight the need for a general positive approach to cybersecurity, evoking and communicating positive emotions. Concerning the dependencies of emotions and attitudes, we found that even minor negative experiences with cybersecurity - such as an unsuccessful update - can result in negative emotions, which in turn can influence the overall affective component towards cybersecurity. In turn, negative experiences, such as an incident experience, can also result in positive attitudes.

7.1.4 Goal 4: Apply Reflections on Emotions as a Method to Reshape how Employees are Viewed and Engaged Within Organizational Cybersecurity Contexts

Organizations have struggled to foster positive cybersecurity behaviors among employees, partly due to a lack of integration of employees' perspectives into cybersecurity practices [13,178]. Papers A and B highlight the importance of emotions in understanding these behaviors. Paper C explores employee involvement in cybersecurity frameworks by leveraging these emotional insights and looking into key points of contact between employees and cybersecurity. Thus, we explore how emotions can be used as a way to improve current views on employees in organizational cybersecurity (RQ4).

RQ4. We identified several key points of contact in relation to the NIST-CSF. Unlike previous research, which primarily concentrated on the "Protect" function (e.g., [21,30,101]), we analyze key points of contact across all NIST-CSF functions. For example, in the "Identify" function, key points include the identification of important contacts and relevant policies. The "Protect" function highlights key areas for preventive measures, such as changing pass-

words, and emphasizes the importance of awareness and training based on various training experiences. The "Detect" function illustrates that employees encounter different threats, while the "Respond" function emphasizes that experiencing cyber incidents provides multiple opportunities to engage with security practices. Additionally, within "Recover", employees interact with improved security measures following an incident. Lastly, we identified organizational factors that extend beyond the functions of the NIST-CSF, such as relationships with security experts. By utilizing emotions as a tool, we identified key points of contact and uncover significant gaps in the NIST-CSF, particularly concerning employee-related aspects, such as emotional recovery and role visibility. Recognizing these gaps provides a foundation for understanding employee perspectives in cybersecurity and for implementing cybersecurity frameworks that take these perspectives into account. This work demonstrates that emotions can serve as a valuable tool for exploring human-centered aspects of cybersecurity.

7.2 Contributions

7.2.1 Theoretical Contribution

Our research leverages the circumplex model of affect [126] to classify cybersecurity-related emotions along valence and arousal dimensions, providing a structured approach to understanding emotional responses. While most literature focuses on single emotions or one affective state (e.g., [21, 30]), our results confirm and extend results by Renaud et al. [136], demonstrating that employees perceive multiple, sometimes contradicting emotions towards cybersecurity. Based on our mapping process, we develop a framework bringing together emotions alongside their causes and consequences including spill-over effects. We, thus, extend the circumplex model by causes and consequences in the field of cybersecurity. We offer insights into a broad variety of causes, directly linked to their corresponding emotions and consequences. This framework, thus, advances theory by offering a more holistic understanding of the emotional landscape surrounding cybersecurity practices.

Contrasting prior research [30,89] and predictions of circumplex models [126,140], interest was not necessarily associated with positive behavioral tendencies and consequences. We argue that this effect is due to the forced compliance paradigm in which a cognitive dissonance emerges from the perceptions of security as boring, while performing mandatory trainings and measures, ultimately resulting in a positive adjustment to security as an interesting topic to counteract the imbalance [55].

The theory of constructed emotions is particularly relevant, suggesting that cybersecurity emotions are not universal responses but are actively constructed based on past experiences, contextual cues, and organizational factors [18]. This theoretical foundation helps explain the diversity and complexity of emotional responses observed in cybersecurity contexts.

For attitudes, the application of the tripartite model of attitudes (affective, cognitive, conative components) [4, 6] offers a comprehensive framework for understanding how em-

ployees form and maintain attitudes towards cybersecurity. We propose a model of attitudes that extends on the previous literature regarding attitudes, primarily emphasizing behavioral tendencies and cognitive evaluations of security behaviors [50, 52, 121]. Our results highlight the necessity for a stronger emphasis on the affective component and cognitive evaluations of security itself, moving beyond merely behavioral tendencies. While most literature views attitudes as a continuum [29, 71, 81, 121, 143], our findings confirm and extend results on attitudinal ambivalence by Ng et al. [113] by revealing components of attitudes that can be contradictory. This recognition of attitudinal components enriches theoretical understandings by showing that employees' attitudes toward cybersecurity are not fixed points on a continuum, but dynamic constellations of affective, cognitive, and conative orientations.

A third contribution advances the understanding of cybersecurity as a fundamentally social phenomenon. While previous research has emphasized the importance of social aspects of cybersecurity [51,64,72], our studies expand on the vital role of social dynamics in shaping attitudes, emotions, and both self and social perceptions. Rather than treating security as purely individual behavior, the findings demonstrate how attitudes and emotions are socially constructed through interactions with colleagues, management, and organizational culture. This social perspective reveals that security behaviors emerge from individual and collective sense-making processes rather than individual rational processes. In doing so, we enhance existing approaches by emphasizing the importance of the relational and cultural contexts in which cybersecurity occurs.

Paper D advances the understanding of cybersecurity by investigating an established framework in the light of human factors. We map traditional technical frameworks (NIST-CSF [114]) to employee perspectives, revealing significant gaps in how existing frameworks address psychological, social, and emotional dimensions of security. By identifying gaps in the NIST-CSF concerning employee aspects, we set a first step towards a shift from technology-centric to human-centered theoretical approaches.

Lastly, our work also makes an important contribution in terms of methodological diversity. We demonstrate the complexity of emotional and attitudinal experiences. We demonstrate the complexity of emotional and attitudinal experiences in cybersecurity by employing a mixed-methods approach that combines tools such as semi-structured interviews, qualitative surveys, verbal and non-verbal measurement tools, and focus groups. Emotions themselves prove to be a valuable tool for accessing experiences in cybersecurity. We encourage future scholars to adopt multi-layered designs incorporating emotional and attitudinal aspects when studying human-centric security processes.

7.2.2 Recommendations for Various Stakeholders

The following section highlights selected recommendations for key stakeholders in cybersecurity, including security experts, organizational management, and academic researchers. These recommendations are grounded both in relevant prior research and the empirical find-

ings presented in this thesis (referenced throughout). They aim to translate the study's insights into actionable guidance for research and practice.

Recommendations for Cybersecurity Practitioners

Address Emotions Appropriately. Our findings indicate that practitioners should aim to first address emotions while reducing emotional dissonance. For instance, through the establishment of an emotion-oriented mindset. Further, high-arousal emotions and subsequent causes should be enhanced following the dependencies revealed in our framework (e.g., an organizational factor: increasing the level of perceived protection (passive) by regularly communicating to the user the efforts of protecting the security infrastructure from the security team/ what is done to keep the employees safe), while considering the risk of undesirable activation i.e. (concealed) insecure behavior and low-arousal emotions and their subsequent causes should be diminished (Paper A).

While we generally advocate for fostering positively valenced emotions due to ethical concerns of evoking negative ones, our research displays complex dynamics on employees' needs for the emotional tone of measures: Although gamification is an established tool for fostering positive engagement in prior literature (e.g., [20, 151]), our research shows that gamification is not necessarily desired by employees (Paper B, C) - which we later also observed in the context of needs for effective cybersecurity education for young adults [163]. This suggests a greater need to focus on making security solutions more user-centered, personalized, or socially accepted rather than simply adding gamified elements. A minority of participants even expressed the view that security should not, or cannot, be made fun, indicating that it should not be gamified (Paper B). They highlight the need to adjust the emotional tone of the content and follow a context-dependent approach (Paper C). Further, there is a wish for transparent communication even if it may evoke fear (Paper C) - yet, excessive fear can lead to avoidance (Paper A) and warrants ethical considerations for which Dupuis et al. have developed an initial set of guidelines [42].

Foster Positive Attitudes. Our research highlights several factors fostering positive attitudes. While some are rather clear in their implementation, others are rather difficult to translate into explicit behavioral strategies. For instance, two factors encompass

1. First, for educational formats, employees requested several types of learning formats (Paper C). Thus, we recommend implementing several types of formats, such as virtual classrooms, workshops in person, consciously implemented gamified elements, user stories for education, videos, cheat sheets, or knowledge databases that have previously proven to be successful (e.g., [124, 147, 151]). Offering this range of formats not only accommodates different learning styles but also sustains engagement by preventing habituation and addressing ambivalent attitudes - where employees recognize cybersecurity's importance yet harbor negative feelings about it.

2. Another example is the approach to security as a process. Here, surveys could screen participants' knowledge, emotions, or attitudes towards cybersecurity and adjust education accordingly. Regular surveys and short assessments can screen participants' understanding and emotional responses, automatically guiding them towards the most relevant next module, whether that be deeper technical training, scenario-based discussions to build self-efficacy, or peer-led reflection sessions. Emerging evidence from related interventions indicates that adaptive, personalized training yields significantly higher engagement and retention than one-size-fits-all approaches [146, 147].

Foster Self-Reflection. Employees' cybersecurity attitudes are deeply shaped by both social experiences and individual perceptions. Even small negative experiences, like frustrations with software updates, can negatively impact their overall feelings about security. This occurs when users mistakenly associate changes in features with security measures (Paper C). Conversely, real incident experiences can boost confidence, yet, risk hindsight bias and overconfidence if memories fade or distort over time (Paper C) [141]. For emotions, self-reflections are generally applied for several uses, such as emotional awareness or emotion regulation [65, 78]. It can help uncover dysfunctional relationships and behaviors as a result of emotions (e.g., procrastination as a result of negative emotions) [45, 154]. Enhancing positive emotions can help mitigate negative ones, but low-arousal positive emotions may lead to undesirable behaviors. To support mental health and resilience, it is important to encourage emotional reflection for a balanced emotional state, particularly in cybersecurity (Paper A). Based on the strong influence of social dynamics in cybersecurity, we recommend integrating both individual and collective reflections.

Foster Social Interactions and Cultivate Psychological Safety Social interactions significantly influence cybersecurity attitudes and behaviors, extending beyond individual cognition to encompass organizational culture and team dynamics [14, 51, 112, 127]. Our findings reveal that employees often fear negative evaluation from colleagues for engaging in security tasks during work hours, creating barriers to communication (Paper A-C). Cultivating a shared team security vision and promoting a positive security mindset can help transform these perceptions and enhance engagement (Paper B-C). Moreover, social interactions, especially conversations about security, foster positive overall security behaviors (Paper B). We later uncovered that social dynamics are particularly relevant for young adults (18-30 years) [163].

To harness positive attitudes and emotions, organizations should facilitate natural security conversations by integrating them into routine workplace settings through initiatives such as security meet-ups, awareness days, and embedding security prompts into shared office materials and communications [174]. Positioning security professionals as approachable rather than isolated experts can bridge the gap between experts and lay users, encouraging inclusive dialogue and knowledge sharing, and overcoming dysfunctional relationships (Paper A-B) [110].

Complementing social facilitation, psychological safety is critical to enabling open communication and risk-taking without fear of blame or reprisal, thereby reducing stress and burnout in high-pressure cybersecurity environments. We recommend promoting psychological safety by modeling inclusive behaviors, creating a blame-free culture that views errors as opportunities for learning, and establishing clear and transparent processes. It is important to be mindful of the emotional impact that transparent communications can have, as they may evoke fear (Papers A and C). This approach aligns with recommendations aimed at fostering guilt rather than shame in response to incidents [134]. Encouraging emotional expression through anonymous channels and supporting mental well-being strengthens resilience and maintains engagement (Paper A).

Finally, fostering a culture that normalizes vulnerability, embraces diverse perspectives, and promotes empathy between users and experts, including storytelling of real-world security experiences, enhances mutual understanding and collective security visions (Paper A, C).

Recommendations for Management

Hire Diverse Security Teams. Research across organizational behavior and innovation processes demonstrates that teams characterized by diversity, be it cultural background, disciplinary training, or cognitive style, consistently outperform homogeneous groups in both creativity and problem-solving capacity [160, 168]. By analogy, cybersecurity stands to gain substantial benefits from forming multidisciplinary security teams that integrate perspectives from computer science, psychology, marketing, communication studies, and other social sciences. Such diversity enriches security understanding with insights into user behavior, enhances the design of emotion-aware communication strategies, and ensures that cultural dimensions, such as norms around privacy and social acceptance of security measures, are fully understood and addressed (Paper A-D). In practice, embedding social scientists and communication experts alongside technical specialists could enrich security awareness campaigns, finely tuned messaging, and employee-centered security integration. Given common financial constraints, organizations could involve such experts not only through full-time positions but also by leveraging existing expertise from departments like marketing or communications.

Be a Role Model. While existing research demonstrates the impact of leadership on security behavior and leadership's impact on coping responses [69, 134], our findings extend these insights by showing that nearly all participants emphasized the critical need for clear management prioritization of cybersecurity (Paper C). While companies often acknowledge the importance of cybersecurity, many participants reported being uncertain about management's actual stance on the matter —sometimes perceiving mixed signals, such as an apparent prioritization of productivity over security (Paper A and C). Thus, participants specifically requested that management actively communicate cybersecurity as a top priority and live the desired security culture through their own actions. Our research further

demonstrates that organizational error culture significantly shapes employee emotions towards security (Paper A), while security conversations enhance overall engagement levels (Paper B). Therefore, to foster positive attitudes and high-arousal positive emotions, we recommend that management serve as role models, cultivate constructive error cultures, and establish psychological safety environments that actively encourage security discussions.

Listen to Your Employees. User participation is fundamentally established within usable system design [95], yet, we found that many employees do not feel included in security processes (Paper A and C). Our findings reveal that employees desire to be integrated into the design and implementation of security processes and measures (Paper B). Many participants expressed experiencing a pronounced lack of autonomy regarding security, leading to negative emotional responses towards cybersecurity requirements (Paper A). Our research further underscores the essential role employees play within cybersecurity frameworks, moving beyond traditional compliance-focused models toward collaborative security governance (Paper D).

We therefore advocate for cultivating an organizational culture of meaningful participation that actively involves diverse stakeholders, including both security specialists and other employees, to foster positive attitudes and high-arousal positive emotions. This participatory approach should encompass multiple levels of engagement, from policy development to implementation planning and ongoing evaluation.

Effective integration could include establishing clear channels for employee feedback, creating cross-functional security committees that include non-technical staff, and implementing regular consultation processes that incorporate employee perspectives into security strategy development.

Recommendations for Researchers

Consider the Complexity of Attitudes and Emotions. Both emotions and attitudes in cybersecurity are multifaceted and often internally contradictory.

Our studies revealed an extensive range of emotions exceeding prior literature, sometimes co-occurring in opposing valences and highly varying in intensity. Consistent with recommendations to capture emotional complexity [53, 128], we advocate employing multiple measurement modalities (e.g., physiological sensors, non-verbal tools, or subjective descriptions) and particularly including subjective tools using open-ended questions to fully represent individuals' emotional experiences.

Attitudes likewise comprise distinct affective, cognitive, and behavioral components that may conflict. We recommend explicitly measuring and reporting each component rather than relying on composite scores. Finally, for both constructs, it is vital to specify the precise object of interest, such as fear of making procedural errors versus fear of external cyber threats, since our findings demonstrate that emotional and attitudinal responses differ depending on their target.

Account for Spill-over Effects and Variety of Behavioral Tendencies. Our results reveal a spectrum of employee cybersecurity behaviors that extend well beyond basic compliance. Consistent with prior research, we identified complex, nontrivial behavioral patterns that surpass simple distinctions like "shadow IT" or rule adherence, reflecting a nuanced set of coping and workaround strategies in response to organizational policies [21,92,159] (Paper A and C). For example, employees may outwardly comply by creating complex passwords, yet undermine security by writing them down and leaving them near their workstations (Paper A). Additionally, behaviors such as procrastinating both security-relevant (e.g., delaying software updates) and security-critical actions (e.g., postponing judgment on suspicious emails) further illustrate this behavioral complexity.

Notably, our data uncover discrepancies between intentions and actual behavior: some employees demonstrate strong policy awareness and intent to comply but hesitate to adopt requirements, while others express intent to follow the rules without actually knowing the content of those policies (Paper A). These findings highlight the limitations of using compliance intentions as a sole indicator of secure behavior. Instead, we recommend including a multi-layered measurement approach, integrating security behaviors, control for concealed insecure behaviors, and incorporating other aspects such as social support seeking.

Extending the work of Dupuis et al. [43], who identified negative long-term effects on security from fear-based interventions, we observed negative spillover effects, such as emotional exhaustion and reduced productivity (Paper A). This suggests that emotion-evoking interventions may achieve positive short-term effects but carry unintended negative consequences over time and beyond the cybersecurity domain. Therefore, we recommend that cybersecurity research recognize the full range of behavioral tendencies and explicitly evaluate long-term and spillover effects.

Incorporate Reflections on Emotions for Detailed Insights into Experiences. Prior emotion research consistently demonstrates that emotional evaluation offers a uniquely powerful lens for understanding complex human experiences, providing depth that goes beyond purely cognitive or behavioral analyses [26, 90]. Our findings confirm and extend this perspective in cybersecurity, revealing that emotional reflections uncover nuanced patterns of user experience, motivation, and vulnerability that standard assessments may overlook. We therefore strongly advocate for adopting an emotional perspective in human-centered cybersecurity research. Incorporating emotional reflection not only enriches the analytic process but also yields actionable insight into the drivers of secure and (concealed) insecure behaviors, making it an essential and transformative tool for understanding human aspects in cybersecurity.

7.3 Limitations and Future Work

It is important to note some limitations of the studies within this doctoral thesis. First, this thesis follows a primarily qualitative approach, which means that the findings are based solely on self-reported data. Despite employing various methods such as interviews, focus groups, and online surveys, this may impact the generalizability of the results. While Paper B offers a broader sample size, future studies could further delve into specific attitudinal and emotional paths and explore the influencing variables for fostering positive attitudes and positive high arousal emotions - both qualitatively and quantitatively.

Second, our research looked into constellations and interdependencies of attitudinal components and emotions. Prior research displays significant effects of attitudinal ambivalence on protection behavior [113]. Thus, future research could investigate constellations of emotions, such as contradicting emotions or the effects of contradicting attitudinal components, such as a positive cognitive component and a negative affective component.

Third, although the context in Paper B was not explicitly defined, some participants focused on their personal lives, while others concentrated on their work environment. Renaud et al. [136] indicate that there may be significant differences between these two contexts in terms of emotional experiences. Further, the authors display that various areas of cybersecurity cause differing emotions - Paper A confirms these results, yet, does not delve into these different fields. Therefore, we recommend that future research separately investigate both contexts, with particular attention to interactions with workplace culture, and explore differences in the various areas of cybersecurity. Further, while Paper C (in comparison to Paper A, B) delved into a single-organization study, prior research indicates interactions of emotions with leadership style [134]. Thus, future studies could explore interactions with the workplace culture.

Fourth, we did not explore attitudes and emotions specific to roles. Prior research indicates that workplace conditions can affect job and security interactions, such as how a cyber attack impacts the perceptions of cybersecurity professionals [152]. Future research could examine role-specific attitudes and emotions, such as those of cybersecurity professionals and management, but also various industries, such as nurses in healthcare, or office workers in finance.

7.4 Conclusion

This doctoral thesis provides a holistic exploration of emotions and attitudes within organizational cybersecurity contexts, emphasizing humans as integral contributors to security rather than the "weakest link." Through four empirical studies employing diverse qualitative methods, it reveals the multifaceted nature of cybersecurity-related emotions, often coexisting and varying widely in intensity, and the complex components that shape employee attitudes. Central findings include frameworks detailing the causes and consequences

of security-related emotions, key factors influencing cybersecurity attitudes, and actionable taxonomies to foster positive attitudes and high-arousal positive emotions.

This thesis underscores the important role of social dynamics and emotional experiences in shaping security behaviors, highlighting the value of culturally and psychologically informed interventions that incorporate peer influence, social support, and communication adapted to the required emotional tone. Mapping employee experiences onto the NIST Cybersecurity Framework exposes critical gaps in policy communication and emotional engagement, calling for a more human-centered, employee-inclusive cybersecurity approach.

By integrating emotional reflections, attitudinal aspects, and social perspectives, this research advances understanding beyond traditional compliance paradigms, offering nuanced insights for security practitioners, management, and researchers. Future work is encouraged to investigate specific stakeholder groups, such as security practitioners themselves, focusing on emotional well-being and fostering psychologically safe workplace environments.

This thesis, thus, contributes foundational knowledge and practical guidance towards embedding knowledge on emotions and attitudes as a cornerstone of effective organizational cybersecurity.

Bibliography

[1] Abroshan, H., Devos, J., Poels, G., and Laermans, E. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *Ieee Access 9* (2021), 121916–121929.

[2] Abun, D., Magallanes, T., Foronda, S. L., and Incarnacion, M. J. Investigation of cognitive and affective attitude of teachers toward research and their behavioral intention to conduct research in the future. *Journal of Humanities and Education Development 1*, 5 (2019), 219–232.

[3] Adams, A., and Sasse, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[4] Ajzen, I. Attitude structure and behavior. In *Attitude structure and function*, The third Ohio State University volume on attitudes and persuasion. Lawrence Erlbaum Associates, Inc, Hillsdale, NJ, US, 1989, pp. 241–274.

[5] Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes 50*, 2 (1991), 179–211.

[6] Ajzen, I. Attitude theory and the attitude-behavior relation. In *New Directions in Attitude Measurement*, D. Krebs and P. Schmidt, Eds. Walter de Gruyter, Berlin, Germany, 1993, pp. 41–57.

[7] Ajzen, I., Fishbein, M., Lohmann, S., and Albarracín, D. The influence of attitudes on behavior. In *The Handbook of Attitudes*, D. Albarracín, B. T. Johnson, and M. P. Zanna, Eds. Lawrence Erlbaum Associates, Mahwah, NJ, USA, 2005, pp. 173–221.

[8] Allianz. Allianz risk barometer 2025: Identifying the major business risks for 2025. `https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf`, 2024. Accessed: September 18, 2025.

[9] Allport, G. W. Attitudes. In *Handbook of Social Psychology*. Clark University Press, Worcester, MA, 1935.

[10] Arnold, D., Blackmon, B., Gibson, B., Moncivais, A. G., Powell, G. B., Skeen, M., Thorson, M. K., and Wade, N. B. The emotional impact of multi-factor authentication for university students. In *ACM CHI Conference on Human Factors in Computing Systems - Extended Abstracts* (New York, NY, USA, 2022), ACM, pp. 1–4.

[11] Azmi, R., Tibben, W., and Win, K. T. Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy 3*, 2 (2018), 258–283.

[12] Bachura, E., Valecha, R., Chen, R., and Rao, H. R. The opm data breach: An investigation of shared emotional reactions on twitter. *MIS Quarterly 46*, 2 (2022).

[13] Bada, M., Sasse, A. M., and Nurse, J. R. C. Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society* (2015).

[14] Bandura, A., and Walters, R. H. *Social learning theory*, vol. 1. Prentice hall Englewood Cliffs, NJ, 1977.

[15] Barrett, L. F. Are emotions natural kinds? *Perspectives on psychological science 1*, 1 (2006), 28–58.

[16] Barrett, L. F. Solving the emotion paradox: categorization and the experience of emotion. *Personality and social psychology review : an official journal of the Society for Personality and Social Psychology, Inc 10*, 1 (2006), 20–46.

[17] Barrett, L. F., Gross, J., Christensen, T. C., and Benvenuto, M. Knowing what you're feeling and knowing what to do about it: Mapping the relation between emotion differentiation and emotion regulation. *Cognition & Emotion 15*, 6 (2001), 713–724.

[18] Barrett, L. F., and Westlin, C. Navigating the science of emotion. In *Emotion measurement*. Elsevier, 2021, pp. 39–84.

[19] Barsalou, L. W. Perceptual symbol systems. *Behavioral and Brain Sciences 22*, 4 (1999), 577–609; discussion 610–60.

[20] Baxter, R. J., Holderness Jr, D. K., and Wood, D. A. Applying basic gamification techniques to it compliance training: Evidence from the lab and field. *Journal of information systems 30*, 3 (2016), 119–133.

[21] Beris, O., Beautement, A., and Sasse, M. A. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (New York, NY, USA, 2015), NSPW '15, Association for Computing Machinery, p. 73–84.

[22] Bilogrevic, I., and Ortlieb, M. " if you put all the pieces together..." attitudes towards data combination and sharing across services and companies. In *Proceedings of the 2016 ACM CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2016), ACM, pp. 5215–5227.

[23] Blythe, J. M., and Coventry, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior 87* (2018), 87–97.

[24] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly 39*, 4 (2015), 837–864.

[25] Breckler, S. J. Empirical validation of affect, behavior, and cognition as distinct components of attitude. *Journal of personality and social psychology 47*, 6 (1984), 1191.

[26] Buchanan, T. W. Retrieval of emotional memories. *Psychological bulletin 133*, 5 (2007), 761.

[27] Buck, R., Khan, M., Fagan, M., and Coman, E. The user affective experience scale: A measure of emotions anticipated in response to pop-up computer warnings. *International Journal of Human–Computer Interaction 34*, 1 (2018), 25–34. `https://doi.org/10.1080/10447318.2017.1314612`.

[28] Budimir, S., Fontaine, J. R., and Roesch, E. B. Emotional experiences of cybersecurity breach victims. *Cyberpsychology, Behavior, and Social Networking 24*, 9 (2021), 612–616.

[29] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* (2010), 523–548.

[30] Burns, A., Roberts, T. L., Posey, C., and Lowry, P. B. The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research 30*, 4 (2019), 1228–1247.

[31] Chen, X., Doublet, S., Sergeeva, A., Lenzini, G., Koenig, V., and Distler, V. What motivates and discourages employees in phishing interventions: An exploration of expectancy-value theory. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (2024), pp. 487–506.

[32] Cheung-Blunden, V., Cropper, K., Panis, A., and Davis, K. Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion 19*, 8 (2019), 1353.

[33] Clore, G. L., Schwarz, N., and Conway, M. Affective causes and consequences of social information processing. *Handbook of social cognition 1* (1994), 323–417.

[34] Conrad, C., Aziz, J., Smith, N., and Newman, A. What Do Users Feel? Towards Affective EEG Correlates of Cybersecurity Notifications. In *NeuroIS Retreat* (2020), Springer, pp. 153–162. https://doi.org/10.1007/978-3-030-60073-0_17.

[35] Cram, W. A., Proudfoot, J. G., and D'Arcy, J. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal 31*, 4 (2021), 521–549.

[36] Da Silva, J., and Jensen, R. B. "cyber security is a dark art": The ciso as soothsayer. *Proc. ACM Hum.-Comput. Interact. 6*, CSCW2 (Nov. 2022).

[37] Davis, F. D. Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS quarterly 13*, 3 (1989), 319–340.

[38] Davis, F. D., Bagozzi, R., and Warshaw, P. Technology acceptance model. *J Manag Sci 35*, 8 (1989), 982–1003.

[39] de Kok, L. C., Oosting, D., and Spruit, M. The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security 46*, 3 (2020), 251–266.

[40] Dinev, T., Goo, J., Hu, Q., and Nam, K. User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal 19*, 4 (2009), 391–412.

[41] Dupuis, M., Jennings, A., and Renaud, K. Scaring people is not enough: An examination of fear appeals within the context of promoting good password hygiene. In *Proceedings of the 22nd Annual Conference on Information Technology Education* (New York, NY, USA, 2021), SIGITE '21, Association for Computing Machinery, p. 35–40.

[42] Dupuis, M., and Renaud, K. Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology 23*, 3 (2021), 265–284.

[43] Dupuis, M., Renaud, K., and Jennings, A. Fear might motivate secure password choices in the short term, but at what cost? In *Hawaii International Conference on System Sciences* (2021).

[44] Eagly, A. H. The psychology of attitudes. *Fort Worth/Harcout Brace Jovanovich College Publishers* (1993).

[45] Eckert, M., Ebert, D. D., Lehr, D., Sieland, B., and Berking, M. Overcome procrastination: Enhancing emotion regulation skills reduce procrastination. *Learning and Individual Differences 52* (2016), 10–18.

[46] Ekman, P. Universals and cultural differences in facial expressions of emotion. In *Nebraska symposium on motivation* (1971), University of Nebraska Press.

[47] Ekman, P. E., and Davidson, R. J. *The nature of emotion: Fundamental questions.* Oxford University Press, 1994.

[48] Fagan, M., Albayram, Y., Khan, M. M. H., and Buck, R. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences 7*, 1 (2017), 1–20. https://doi.org/10.1186/s13673-017-0093-6.

[49] Fagan, M., Khan, M. M. H., and Buck, R. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior 51* (2015), 504–519.

[50] Faklaris, C., Dabbish, L., and Hong, J. I. Do they accept or resist cybersecurity measures? development and validation of the 13-item security attitude inventory (sa-13), 2022.

[51] Faklaris, C., Dabbish, L., and Hong, J. I. A framework for reasoning about social influences on security and privacy adoption. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2024), CHI EA '24, Association for Computing Machinery.

[52] Faklaris, C., Dabbish, L. A., and Hong, J. I. A self-report measure of end-user security attitudes (sa-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (Berkeley, CA, 2019), USENIX Association, pp. 61–77.

[53] Feldman-Barrett, L. *How emotions are made: The secret life of the brain.* Pan Macmillan, 2017.

[54] Festinger, L. *A Theory of Cognitive Dissonance.* Stanford University Press, Stanford, CA, 1957.

[55] Festinger, L., and Carlsmith, J. M. Cognitive consequences of forced compliance. *The journal of abnormal and social psychology 58*, 2 (1959), 203.

[56] Fishbein, M., and Ajzen, I. *Belief, attitude, intention and behaviour: An introduction to theory and research.* Addison-Wesley, Reading, MA, 1975.

[57] Frijda, N. H. The laws of emotion. *American Psychologist 43*, 5 (1988), 349–358. https://doi.org/10.1037/0003-066X.43.5.349.

[58] Frijda, N. H. Moods, emotion episodes, and emotions. In *Handbook of emotions.* The Guilford Press, New York, NY, US, 1993, pp. 381–403.

[59] Frijda, N. H., Kuipers, P., and ter Schure, E. Relations among emotion, appraisal, and emotional action readiness. *Journal of Personality and Social Psychology 57*, 2 (1989), 212–228.

[60] Fruchter, N., and Liccardi, I. Consumer attitudes towards privacy and security in home assistants. In *Proceedings of the 2018 ACM CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2018), ACM, pp. 1–6.

[61] Fulton, K. R., Gelles, R., McKay, A., Abdi, Y., Roberts, R., and Mazurek, M. L. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security* (Santa Clara, CA, USA, Aug. 2019), SOUPS 2019, USENIX Association, pp. 79–95. `https://www.usenix.org/conference/soups2019/presentation/fulton`.

[62] Gabriele, S., and Chiasson, S. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 ACM CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2020), ACM, pp. 1–12.

[63] George, J. M. Trait and state affect. *Individual differences and behavior in organizations 1* (1996), 145–171.

[64] Gerber, N., and Marky, K. The nerd factor: The potential of s&p adepts to serve as a social resource in the user's quest for more secure and privacy-preserving behavior. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (Berkely, CA, USA, 2022), Usenix, pp. 57–76.

[65] Grecucci, A., Pappaianni, E., Siugzdaite, R., Theuninck, A., and Job, R. Mindful emotion regulation: Exploring the neurocognitive mechanisms behind mindfulness. *BioMed research international 2015*, 1 (2015), 670724.

[66] Greenaway, K. H., Kalokerinos, E. K., and Williams, L. A. Context is everything (in emotion research). *Social and Personality Psychology Compass 12*, 6 (2018), 1–18.

[67] Greenwald, A. G., McGhee, D. E., and Schwartz, J. L. Measuring individual differences in implicit cognition: the implicit association test. *Journal of personality and social psychology 74*, 6 (1998), 1464.

[68] Gross, J. J., and Feldman Barrett, L. Emotion generation and emotion regulation: One or two depends on your point of view. *Emotion review 3*, 1 (2011), 8–16.

[69] Guhr, N., Lebek, B., and Breitner, M. H. The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal 29*, 2 (2019), 340–362.

[70] Gulenko, I. Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security 22*, 2 (2014), 167–178.

[71] Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems 28*, 2 (2011), 203–236.

[72] Haney, J. M., and Lutters, W. G. "it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (Baltimore, MD, Aug. 2018), USENIX Association, pp. 411–425.

[73] Heider, F. Attitudes and cognitive organization. *The Journal of psychology 21*, 1 (1946), 107–112.

[74] Heider, F. *The psychology of interpersonal relations*. Psychology Press, 1958.

[75] Henerson, M. E., Morris, L. L., and Fitz-Gibbon, C. T. *How to measure attitudes*, vol. 6. Sage, 1987.

[76] Herath, T., and Rao, H. R. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems 18*, 2 (2009), 106–125.

[77] Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, A., Acar, Y., and Dürmuth, M. A world full of privacy and security (mis) conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 ACM CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2023), ACM, pp. 1–23.

[78] Herwig, U., Kaffenberger, T., Jäncke, L., and Brühl, A. B. Self-related awareness and emotion regulation. *NeuroImage 50*, 2 (2010), 734–741.

[79] Hielscher, J., Menges, U., Parkin, S., Kluge, A., and Sasse, M. A. "employees who don't accept the time security takes are not aware enough": The ciso view of human-centred security. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA, Aug. 2023), USENIX Association, pp. 2311–2328.

[80] Hoemann, K., Nielson, C., Yuen, A., Gurera, J. W., Quigley, K. S., and Barrett, L. F. Expertise in emotion: A scoping review and unifying framework for individual differences in the mental representation of emotional experience. *Psychological Bulletin 147*, 11 (Nov. 2021), 1159–1183.

[81] Hu, Q., Dinev, T., Hart, P., and Cooke, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences 43*, 4 (2012), 615–660.

[82] Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management 51*, 1 (2014), 69–79.

[83] Isen, A. M. Toward understanding the role of affect in cognition. In *Handbook of Social Cognition*, R. R. Wyer and T. K. Srull, Eds., vol. 3. Lawrence Erlbaum Associates, Mahwah, NJ, 1984, pp. 179–236.

[84] Izard, C. E. Four systems for emotion activation: cognitive and noncognitive processes. *Psychological review 100*, 1 (1993), 68.

[85] Johnson-Laird, P. N. *Mental models: Towards a cognitive science of language, inference, and consciousness*, 6. print ed., vol. 6 of *Cognitive science series*. Harvard Univ. Press, Cambridge, 1995.

[86] Johnston, A. C., and Warkentin, M. Fear appeals and information security behaviors: An empirical study. *MIS quarterly 34*, 3 (2010), 549–566.

[87] Jones, N. A., Ross, H., Lynam, T., Perez, P., and Leitch, A. Mental models: An interdisciplinary synthesis of theory and methods. *Ecology and Society 16*, 1 (2011), 1–13.

[88] Kahneman, D. *Thinking, fast and slow*. macmillan, 2011.

[89] Kam, H.-J., Ormond, D. K., Menard, P., and Crossler, R. E. That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal 32*, 4 (2022), 888–926.

[90] Kensinger, E. A. Remembering the details: Effects of emotion. *Emotion review 1*, 2 (2009), 99–113.

[91] Khoo, Y. X., Kang, R. M., Reynolds, T. L., and Mentis, H. M. "that's kind of sus (picious)": The comprehensiveness of mental health application users' privacy and security concerns. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2024), ACM, pp. 1–16.

[92] Kirlappos, I., Parkin, S., and Sasse, M. A. Learning from "shadow security:" why understanding non-compliant behaviors provides the basis for effective security. In *Proceedings 2014 Workshop on Usable Security* (Reston, VA, February 23, 2014), M. Smith and D. Wagner, Eds., Internet Society.

[93] Krombholz, K., Busse, K., Pfeffer, K., Smith, M., and von Zezschwitz, E. "if https were secure, i wouldn't need 2fa" - end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)* (San Francisco, CA, 2019), IEEE, pp. 246–263.

[94] Krosnick, J., Judd, C., and Wittenbrink, B. Attitude measurement. *Handbook of attitudes and attitude change* (2005), 21–76.

[95] Kujala, S. User involvement: a review of the benefits and challenges. *Behaviour & information technology 22*, 1 (2003), 1–16.

[96] Lafontaine, E., Sabir, A., and Das, A. Understanding people's attitude and concerns towards adopting iot devices. In *Proceedings of the 2021 ACM CHI Conference on Human Factors in Computing Systems - Extended Abstracts* (New York, NY, USA, 2021), ACM, pp. 1–10.

[97] Lazarus, R. S. *Emotion and adaptation*. Oxford University Press, Oxford, UK, 1991.

[98] Lazarus, R. S., and Folkman, S. *Stress, appraisal, and coping*. Springer publishing company, 1984.

[99] Lennartsson, M., Kävrestad, J., and Nohlberg, M. Exploring the meaning of usable security–a literature review. *Information & Computer Security 29*, 4 (2021), 647–663.

[100] Levenson, R. W. Human emotion: A functional view. *The nature of emotion: Fundamental questions 1* (1994), 123–126.

[101] Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. A. What users do besides problem-focused coping when facing it security threats: An emotion-focused coping perspective. *MIS quarterly 43*, 2 (2019), 373–394.

[102] Likert, R. A technique for the measurement of attitudes. *Archives of psychology* (1932).

[103] Lindquist, K. A., and Barrett, L. F. Constructing emotion: The experience of fear as a conceptual act. *Psychological science 19*, 9 (2008), 898–903.

[104] Lindquist, K. A., Wager, T. D., Kober, H., Bliss-Moreau, E., and Barrett, L. F. The brain basis of emotion: a meta-analytic review. *Behavioral and brain sciences 35*, 3 (2012), 121–143.

[105] Lord, C. G., Hill, S. E., Holland, C. J., Yoke, K., and Lu, T. Attitudes: An evolutionary perspective. In *Evolutionary perspectives on social psychology*. Springer, New York, NY, 2015, pp. 177–187.

[106] Lutz, C. A. *Unnatural Emotions: Everyday Sentiments on a Micronesian Atoll and Their Challenge to Western Theory*. University of Chicago Press, Chicago, 1988.

[107] Maithri, M., Raghavendra, U., Gudigar, A., Samanth, J., Barua, P. D., Murugappan, M., Chakole, Y., and Acharya, U. R. Automated emotion recognition: Current trends and future perspectives. *Computer Methods and Programs in Biomedicine* (2022), 106646. https://doi.org/10.1016/j.cmpb.2022.106646.

[108] Martin, L. L., Ward, D. W., Achee, J. W., and Wyer, R. S. Mood as input: People have to interpret the motivational implications of their moods. *Journal of Personality and Social Psychology 64*, 3 (1993), 317—-326. https://doi.org/10.1037/0022-3514.64.3.317.

[109] Massumi, B. The autonomy of affect. *Cultural Critique*, 31 (1995), 83.

[110] Menges, U., Hielscher, J., Buckmann, A., Kluge, A., Sasse, M. A., and Verret, I. Why it security needs therapy. In *Computer Security. ESORICS 2021 International Workshops* (Cham, 2022), Springer eBook Collection, Springer International Publishing and Imprint Springer, pp. 335–356.

[111] Moody, G. D., Siponen, M., and Pahnila, S. Toward a unified model of information security policy compliance. *MIS quarterly 42*, 1 (2018), 285–A22.

[112] Moore, L., Mori, T., and Hasegawa, A. A. Negative effects of social triggers on user security and privacy behaviors. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (Berkely, CA, USA, 2024), Usenix, pp. 605–622.

[113] Ng, K. C., Zhang, X., Thong, J. Y., and Tam, K. Y. Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of management information systems 38*, 3 (2021), 732–764.

[114] NIST (National Institute of Standards and Technology). Framework for improving critical infrastructure cybersecurity, 2014.

[115] NIST (National Institute of Standards and Technology). Framework for improving critical infrastructure cybersecurity, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[116] NIST (National Institute of Standards and Technology). The nist cybersecurity framework (csf) 2.0. NIST Cybersecurity White Paper (CSWP) NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024.

[117] NIST (National Institute of Standards and Technology). Human-centered cybersecurity. https://csrc.nist.gov/projects/human-centered-cybersecurity, 2025. Accessed: 2025-09-17.

[118] NordPass. How many passwords does the average person have? https://nordpass.com/blog/how-many-passwords-does-average-person-have/, 2024. Accessed: 2025-09-17.

[119] Norman, D. A. Some observations on mental models. In *Mental models*. Psychology Press, Los Altos, CA, 2014, pp. 15–22.

[120] Osgood, C. E., Suci, G. J., and Tannenbaum, P. H. *The measurement of meaning*. No. 47. University of Illinois press, 1957.

[121] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security 66* (2017), 40–51.

[122] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security 42* (2014), 165–176. `https://doi.org/10.1016/j.cose.2013.12.003`.

[123] Petty, R. E., and Cacioppo, J. T. The elaboration likelihood model of persuasion. In *Advances in experimental social psychology*, vol. 19. Elsevier, 1986, pp. 123–205.

[124] Pfeffer, K., Mai, A., Weippl, E., Rader, E., and Krombholz, K. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (Boston, MA, USA, Aug. 2022), USENIX Association, pp. 1–18. `https://www.usenix.org/conference/soups2022/presentation/pfeffer`.

[125] Pham, H. C., Brennan, L., and Furnell, S. Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications 46* (2019), 96–107.

[126] Posner, J., Russell, J. A., and Peterson, B. S. The circumplex model of affect: An integrative approach to affective neuroscience, cognitive development, and psychopathology. *Development and psychopathology 17*, 3 (2005), 715–734.

[127] Prislin, R., and Wood, W. Social influence in attitudes and attitude change: the role of social consensus on attitudes and attitude change. In *Handbook of Attitudes*, D. Albarracín, B. T. Johnson, and M. P. Zanna, Eds. Psychology Press, Mahwah, NJ, US, 2014, pp. 671 – 706.

[128] Quigley, K. S., Lindquist, K. A., and Barrett, L. F. Inducing and measuring emotion and affect: Tips, tricks, and secrets. *Handbook of research methods in social and personality psychology 220* (2014), 252.

[129] Rader, E., Wash, R., and Brooks, B. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (New York, NY, USA, 2012), SOUPS '12, Association for Computing Machinery.

[130] Redmiles, E. M., Malone, A. R., and Mazurek, M. L. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)* (San Jose, CA, 2016), IEEE, pp. 272–288.

[131] Reeves, A., Delfabbro, P., and Calic, D. Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open 11*, 1 (2021), 21582440211000049.

[132] Renaud, K., and Dupuis, M. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the new security paradigms workshop* (New York, NY, USA, 2019), ACM, pp. 42–56.

[133] Renaud, K., and Flowerday, S. Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications 34* (2017), 76–81.

[134] Renaud, K., Searle, R., and Dupuis, M. Shame in cyber security: effective behavior modification tool or counterproductive foil? In *Proceedings of the 2021 New Security Paradigms Workshop* (New York, NY, USA, 2021), ACM, pp. 70–87.

[135] Renaud, K., Zimmerman, V., Maguire, J., and Draper, S. Lessons learned from evaluating eight password nudges in the wild. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)* (2017), pp. 25–37.

[136] Renaud, K., Zimmermann, V., Schürmann, T., and Böhm, C. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications 8*, 1 (2021), 1–17.

[137] Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., and Pal, D. Enhancing cybersecurity resilience: A comprehensive analysis of human factors and security practices aligned with the nist cybersecurity framework. In *Proceedings of the 13th International Conference on Advances in Information Technology* (2023), pp. 1–16.

[138] Roseman, I. J. Appraisal determinants of discrete emotions. *Cognition & Emotion 5*, 3 (1991), 161–200.

[139] Roseman, I. J., Wiest, C., and Swartz, T. S. Phenomenology, behaviors, and goals differentiate discrete emotions. *Journal of Personality and Social Psychology 67*, 2 (1994), 206–221.

[140] Russell, J. A. A circumplex model of affect. *Journal of personality and social psychology 39*, 6 (1980), 1161.

[141] Russo, J. E., Schoemaker, P. J., et al. Managing overconfidence. *Sloan management review 33*, 2 (1992), 7–17.

[142] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. Information security conscious care behaviour formation in organizations. *Computers & Security 53* (2015), 65–78.

[143] Safa, N. S., Von Solms, R., and Furnell, S. Information security policy compliance model in organizations. *computers & security 56* (2016), 70–82.

[144] Sasse, M. A., and Flechais, I. *Usable Security: Why Do We Need It? How Do We Get It?* Security and Usability: Designing secure systems that people can use. O'Reilly, Sebastopol, US, 2005.

[145] Schneier, B. *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2015.

[146] Schöni, L., Carles, V., Strohmeier, M., Mayer, P., and Zimmermann, V. You know what? - evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. In *Proceedings of the 2024 European Symposium on Usable Security* (New York, NY, USA, 2024), ACM, pp. 1–14.

[147] Schöni, L., Roch, N., Sievers, H., Strohmeier, M., Mayer, P., and Zimmermann, V. It's a match-enhancing the fit between users and phishing training through personalisation. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (2025), pp. 1–25.

[148] Schwarz, N., and Clore, G. L. Feelings and phenomenal experiences. In *Social psychology: Handbook of basic principles, 2nd ed.* The Guilford Press, New York, NY, US, 2007, pp. 385–407.

[149] Security, I. Cost of a data breach report 2025, 2024.

[150] Shouse, E. Feeling, emotion, affect. *M/c journal 8*, 6 (2005).

[151] Silic, M., and Lowry, P. B. Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems 37*, 1 (2020), 129–161.

[152] Singh, T., Johnston, A. C., D'Arcy, J., and Harms, P. D. Stress in the cybersecurity profession: a systematic review of related literature and opportunities for future research. *Organizational Cybersecurity Journal: Practice, Process and People 3*, 2 (2023), 100–126.

[153] Siponen, M., Mahmood, M. A., and Pahnila, S. Employees' adherence to information security policies: An exploratory field study. *Information & management 51*, 2 (2014), 217–224.

[154] Sirois, F. M. Procrastination and stress: A conceptual review of why context matters. *International Journal of Environmental Research and Public Health 20*, 6 (2023), 5031.

[155] Skiendziel, T., Rösch, A. G., and Schultheiss, O. C. Assessing the convergent validity between the automated emotion recognition software Noldus FaceReader 7 and Facial Action Coding System Scoring. *PloS One 14*, 10 (2019), e0223905. `https://doi.org/10.1371/journal.pone.0223905`.

[156] Statista. Forecast: Cost of cybercrime worldwide. `https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide`, 2025. Accessed: 2025-09-27.

[157] Svenningsson, J., Höst, G., Hultén, M., and Hallström, J. Students' attitudes toward technology: exploring the relationship among affective, cognitive and behavioral components of the attitude construct. *International Journal of Technology and Design Education 32*, 3 (2022), 1531–1551.

[158] Syafrizal, M., Selamat, S. R., and Zakaria, N. A. Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security 12*, 3 (2020), 417–432.

[159] Van Acken, J.-P., Jansen, F., Jansen, S., and Labunets, K. Who is the it department anyway: An evaluative case study of shadow it mindsets among corporate employees. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (2024), pp. 527–545.

[160] Van Knippenberg, D., Van Ginkel, W. P., and Homan, A. C. Diversity mindsets and the performance of diverse teams. *Organizational Behavior and Human Decision Processes 121*, 2 (2013), 183–193.

[161] van Schaik, P., Renaud, K., Wilson, C., Jansen, J., and Onibokun, J. Risk as affect: The affect heuristic in cybersecurity. *Computers & Security 90* (2020), 101651. `https://doi.org/10.1016/j.cose.2019.101651`.

[162] Volkamer, M., and Renaud, K. Mental models–general introduction and review of their application to human-centred security. In *Number theory and cryptography: Papers in honor of johannes buchmann on the occasion of his 60th birthday*. Springer, Berlin, Heidelberg, 2013, pp. 255–280.

[163] von Preuschen, A., Amend, Y. N., Henke, R., Wrede, L., Schuhmacher, M. C., and Zimmermann, V. Climbing towers or looking at flowers: Exploring young adults' needs for effective cybersecurity education through design thinking and lego serious play. In *Mensch und Computer 2025-Workshopband* (2025), Gesellschaft für Informatik eV, pp. 10–18420.

[164] von Preuschen, A., Zimmermann, V., and Schuhmacher, M. How do you Feel about Cybersecurity? – A Literature Review on Emotions in Cybersecurity. In *Proceedings of the International Symposium on Technikpsychologie (TecPsy)* (2023), N. Gerber and V. Zimmermann, Eds., Sciendo. https://sciendo.com/book/9788366675896.

[165] von Preuschen, A., Zimmermann, V., and Schuhmacher, M. C. How do you feel about cybersecurity?–a literature review on emotions in cybersecurity. In *International Symposium on Technikpsychologie (TecPsy) 2023* (Darmstadt, Germany, 2023), Sciendo, pp. 1–13.

[166] Walther, E., Nagengast, B., and Trasselli, C. Evaluative conditioning in social psychology: Facts and speculations. *Cognition and emotion 19*, 2 (2005), 175–196.

[167] Walther, E., Weil, R., and Düsing, J. The role of evaluative conditioning in attitude formation. *Current Directions in Psychological Science 20*, 3 (2011), 192–196.

[168] Wang, J., Cheng, G. H.-L., Chen, T., and Leung, K. Team creativity/innovation in culturally diverse teams: A meta-analysis. *Journal of Organizational Behavior 40*, 6 (2019), 693–708.

[169] Wash, R. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (New York, NY, USA, 2010), ACM, pp. 1–16.

[170] Watson, D., and Clark, L. A. The panas-x: Manual for the positive and negative affect schedule-expanded form.

[171] Weiss, R. F. Persuasion and the acquisition of attitudes: Models from conditioning and selective learning. *Psychological Reports 11*, 3 (1962), 709–732.

[172] Whitten, A., and Tygar, J. D. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium* (1999), vol. 348, pp. 169–184.

[173] Wu, J., and Zappala, D. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (Baltimore, MD, Aug. 2018), USENIX Association, pp. 395–409.

[174] Wu, Y., Edwards, W. K., and Das, S. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)* (2022), pp. 1863–1879.

[175] Zanna, M. P., and Rempel, J. K. Attitudes: A new look at an old concept. In *Attitudes: Their structure, function, and consequences*, Key readings in social psychology. Psychology Press, New York, NY, US, 2008, pp. 7–15.

[176] Zhang, X. A., and Borden, J. How to communicate cyber-risk? an examination of behavioral recommendations in cybersecurity crises. *Journal of Risk Research 23*, 10 (2020), 1336–1352.

[177] Zielinska, O., Welk, A., Mayhorn, C. B., and Murphy-Hill, E. Exploring expert and novice mental models of phishing. In *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security* (2015), pp. 1–2.

[178] Zimmermann, V., and Renaud, K. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies 131* (2019), 169–187.

[179] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems 62*, 1 (2022), 82–97.

Affidavit

I hereby declare that I completed the papers submitted and listed hereafter independently and with only those forms of support mentioned in the relevant paper or in the following supplementary list. When working with the authors listed, I contributed no less than a proportionate share of the work. In the analyses that I have conducted and to which I refer in the papers, I have followed the principles of good academic practice, as stated in the Statute of Justus Liebig University Giessen for ensuring good scientific practice.

Ich erkläre hiermit, dass ich die vorgelegten und nachfolgend aufgelisteten Aufsätze selbstständig und nur mit den Hilfen angefertigt habe, die im jeweiligen Aufsatz angegeben oder zusätzlich in der nachfolgenden Liste aufgeführt sind. In der Zusammenarbeit mit den angeführten Koautoren war ich mindestens anteilig beteiligt. Bei den von mir durchgeführten und in den Aufsätzen erwähnten Untersuchungen habe ich die Grundsätze guter wissenschaftlicher Praxis, wie sie in der Satzung der Justus-Liebig-Universität Gießen zur Sicherung guter wissenschaftlicher Praxis niedergelegt sind, eingehalten.

Date:

Signature:

List of Papers

1. Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. 2024. Beyond Fear and Frustration - Towards a Holistic Understanding of Emotions in Cybersecurity. In Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). USENIX Association, Philadelphia, PA, 623–642.

2. Nina Gerber, Verena Zimmermann, Alexandra von Preuschen, and Karen Renaud. 2025. Unpacking the social and emotional dimensions of security and privacy user engagement. In Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025). USENIX Association, Seattle. 535-554.

3. Alexandra von Preuschen, Carolin Benda, Monika C. Schuhmacher, and Verena Zimmermann. 2025. Fear, Fun or None: A Qualitative Quest Towards Unlocking Cybersecurity Attitudes. In CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 24 pages.

4. Alexandra von Preuschen, Roman Henke, Manpreet Kaur, Julian Nickel, and Monika C. Schuhmacher. 2025, in press. Towards an Employee-Centric Framework of Cybersecurity. In European Symposium on Usable Security (EuroUSEC 2025), Manchester, UK.