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

Alexandra von Preuschen and Monika C. Schuhmacher,
Justus-Liebig-University Gießen; Verena Zimmermann, *ETH Zurich*

https://www.usenix.org/conference/soups2024/presentation/von-preuschen

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

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 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.

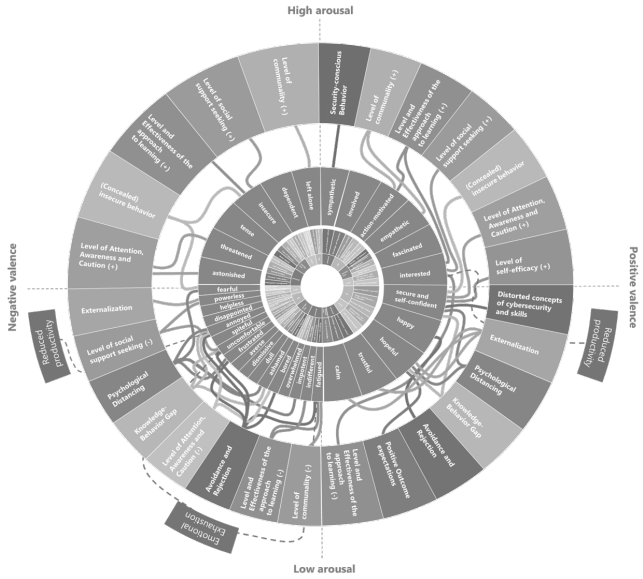

Figure 1: Eye of cybersecurity-related emotions. See digital appendix A (linked in Appendix A) for a larger color version.

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

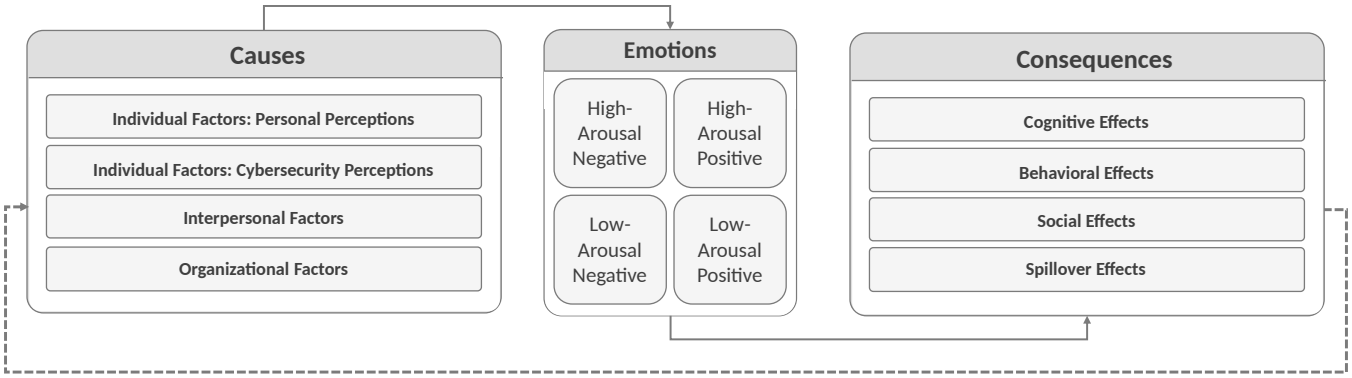

Figure 2: Framework of emotions in cybersecurity

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.