Managing Organizational Cyber Security – The Distinct Role of Internalized Responsibility

Stefan Faltermaier
University of Passau
stefan.faltermaier@uni-passau.de

Kim Strunk
University of Passau
kim.strunk@uni-passau.de

Michaela Obermeier
University of Passau
michaela.obermeier@uni-passau.de

Marina Fiedler
University of Passau
marina.fiedler@uni-passau.de

Abstract

Desirable user behavior is key to cyber security in organizations. However, a comprehensive overview on how to manage user behavior effectively, in order to support organizational cyber security, is missing. Building on extant research to identify central components of organizational cyber security management and on a qualitative analysis based on 20 semi-structured interviews with users and IT-Managers of a European university, we present an integrated model on this issue. We contribute to understanding the interrelations of namely user awareness, user IT-capabilities, organizational IT, user behavior, and especially internalized responsibility and relation to organizational cyber security.

Keywords: Cyber Security, User Behavior, Internalization of Responsibility, User Awareness

1. Introduction

Cyber security describes the targeted use of resources and digital structures to protect cyber processes and systems and their environment (Craigen et al., 2014). The concept also includes the protection of users and their digital property as well as their digital information, data, and assets (Von Solms & Van Niekerk, 2013). Cyber security thus goes beyond the underlying concept of information security, which is only concerned with the protection of information resources. Due to rapid digitization and technological change, managing cyber security effectively has become an increasingly important issue for organizations. However, in parallel to valuable opportunities, rapid technological innovations are also constantly creating additional cyber threats (Deloitte, 2021; Pan & Yang, 2018). Along the number of digital threats, the number of successful attacks and the resulting damages increase (Sen, 2018). Last year, over 90% of companies were affected by a malicious cyber-attack (Bitkom, 2021) and the financial damage caused by ransomware alone amounted to $20 trillion (Braue, 2021).

In recent years, this continuing upward trend was further reinforced by the Covid19 pandemic, in which increased digital usage times and more remote work drastically increased the number of potential security risks and thus the overall cyber security risk (Lallie et al., 2021). Albeit, this is a well-known problem, effective management of these issues still lacks in many organizations (Bada et al., 2015).

Considering the socio-technical nature of cyber security, it’s often argued that purely technical solutions can hardly make up successful cyber security strategies (Furnell et al., 2007; McCormac et al., 2017; Parsons et al., 2014). This seems especially illusive as users are often labeled the weakest link in this context (Corradini & Nardelli, 2018; Culnan et al., 2008; de Bruijn & Janssen, 2017; Sankaranarayanan et al., 2007). User behaviors such as inaccuracy, lack of concentration, and ignorance often undermine even the most sophisticated technical security measures (Corradini & Nardelli, 2018; Culnan et al., 2008; Hong, 2012).

Managing user behavior is thus key for cyber security in organizations. Literature on different aspects of this issue is rich. Comprising for example strands on the central role of user awareness (Bulgurcu et al., 2010; Corradini & Nardelli, 2018; Culnan et al., 2008; D´Arcy et al., 2009; Macabante et al., 2019; Spears & Barki, 2010), user responsibility (de Bruijn & Janssen, 2017; Filipczuk et al., 2019; LaRose et al., 2008), or the impact of different types of organizations (Acuna et al., 2021; Balozian & Leidner, 2017). Still, we lack a comprehensive understanding of users’ cyber security behavior (Chen et al., 2021; Jenkins et al., 2021) and especially the interrelations of the different building blocks of organizational cyber security management. To fill this void, we ask: *How are the different components of organizational cyber security interrelated and how do they benefit desirable user behavior?*

URI: https://hdl.handle.net/10125/103373
978-0-9981331-6-4

We aim to answer this question from a user and an IT-Manager perspective. We build our study on extant literature as well as qualitative data from semi-structured interviews. We develop a comprehensive model to illustrate the most important building blocks of organizational cyber security management and describe the interrelations of these building blocks. Our results show, how user awareness and user IT-capabilities build the basis for the internalizing responsibility, which benefits organizational cyber security. Particularly, internalized responsibility is a key prerequisite for and has a positive influence on desirable user behavior.

2. Research Background

2.1. Organizational users and cyber security

In line with extant Information Systems (IS) -research we understand cyber security as a socio-technical phenomenon (Acuna et al., 2021; Craigen et al., 2014; Culnan et al., 2008; Macabante et al., 2019) insofar that we agree that neither a pure technological nor a pure human-centered view can help to fully understand the phenomenon. However, we also agree with IS-scholars stressing the distinct role of users and their behavior in regard to cyber security (Corradini & Nardelli, 2018; Culnan et al., 2008; de Bruijn & Janssen, 2017; Sankaranarayanan et al., 2007) as they argue that even the security of systems, guarded by highly sophisticated technical measures, is dependent on the way users use these systems. In contrast to soft- and hardware, users cannot be fully surveilled for legal, ethical, and technical reasons, nor can they be updated easily after potential risks are detected. This hinders detection and prevention of cyber security breaches caused by misperception, misbehavior or inattention in users' behavior. Consequently, users are a weak link in the metaphorical chain of cyber security (Corradini & Nardelli, 2018; Culnan et al., 2008; de Bruijn & Janssen, 2017; Von Skarczinski et al., 2022). Thus, practitioners and scholars increasingly focus on training and development to alter user behavior and eventually to improve cyber security (Bulgurcu et al., 2010; Culnan et al., 2008; de Bruijn & Janssen, 2017; Spears & Barki, 2010). In sum, IS literature on cyber security underlines the importance of user behavior for cyber security.

Besides the central role of the user, literature stresses the importance of different contexts in which cyber security is researched (Balozian & Leidner, 2017). In this study we focus on an organizational context. Scholars frequently research cyber security in organizational settings. (Corradini & Nardelli, 2018; Culnan et al., 2008; Filipczuk et al., 2019; Macabante et al., 2019; Pahnila et al., 2007; Parsons et al., 2014). This context is characterized by a formal relationship of an organization and its employees who use the organizational IT. The users are endowed with rights and obligations in relation to the use of organizational IT and both parties are involved in the development and implementation of a cyber security strategy. Context factors can differ between different organizations or types of organizations. For example, resources that are available for cyber security management (e.g., cyber security-training and education, measures to deter undesirable user behavior and to reward desired behavior) vary depending on size, industry or purpose of an organization (Acuna et al., 2021).

2.2. Organizational cyber security management

The component most frequently referred to, in relation to cyber security management, is awareness. Awareness depends on all the user's general and specific knowledge about cyber dangers and counteractive security measures (Bulgurcu et al., 2010; Culnan et al., 2008; Dinev & Hu, 2007; Pahnila et al., 2007; Parsons et al., 2014). To be able to act in a security-oriented manner, the user first needs a knowledge base about the field in which he or she is operating. Many studies therefore recommend improving user knowledge through targeted information and training measures that educate users about the subject (Balozian & Leidner, 2017; Pahnila et al., 2007). Expanding knowledge can preventively ensure that users are more aware of potential dangers at an early stage and are thus better informed in advance (Balozian & Leidner, 2017). However, Aggarwal and colleagues (2015) point out that users often have a strong mismatch between actual and self-assessed knowledge about cyber security. This often leads to users overestimating their own abilities and not actively seeking to expand their knowledge.

Besides awareness, users' capabilities in using IT are a crucial component of organizational cyber security management (Ani et al., 2019; Workman et al., 2008). Without being able to react properly to hazardous situations, users cannot actively support organizational cyber security. To improve these capabilities, targeted training of users' practical knowledge to provide them with know-how about applicable practices for preventing or dealing with hazardous situations is needed (Balozian & Leidner, 2017).

Besides awareness and IT capabilities, responsibility is a frequently addressed component in the literature. Siponen (2000) introduced the term prescriptive awareness, describing a mixture of role responsibility and moral responsibility. This means, being responsible for one's own digital actions and taking responsibility for demonstrating safe behavior, such as incorporating security measures (Dinev & Hu, 2007). In order to support such desirable user behavior, IT managers can take measures to impose responsibility on users externally. In this regard, measures to influence users' motivation play a central role (Herath & Rao, 2009), essentially comprising measures to deter undesired, security non-compliant behavior, through sanctions like reprimands (D´Arcy et al., 2009), and measures to reward desired behavior, e.g., through monetary awards. Thereby, deterrence measures aim at increasing cost of noncompliance, making this kind of behavior less attractive for individuals, and rewards aim at increasing benefits of compliant behavior, making such behavior more attractive (Bulgurcu et al., 2010). Further, based on the results of their study, De Bruijin and Janssen (2017) advocate for shared responsibility between users and higher hierarchical levels and emphasize that shared responsibility for cyber security leads to better implementation of digital security measures. LaRose and colleagues (2008) show that users who saw safe behavior as their personal responsibility also showed much higher compliance than users who did not see themselves as responsible for safe behavior. Filipczuk and colleagues (2019) confirm these findings as users assigned with a high level of responsibility for their own digital behavior easily adopted it and acted according to security guidelines. Both studies (Filipczuk et al., 2019; LaRose et al., 2008) showed that personal responsibility plays an important role in improving user behavior.

Albeit, the aforementioned components are frequently discussed in literature, their interrelations with each other, their impact on user behavior and their integration into an overall model for organizational cyber security management are missing. To address this void in extant research, we conducted a qualitative study in a case organization, whereby we asked the participants for these interrelations.

3. Methodology

To gain insights on how the different components of organizational cyber security management are interrelated and how they link to desirable user behavior, we conducted a qualitive case study. This method allows for the observation and understanding of underlying mechanisms and relationships (Eisenhardt, 1989; Gioia et al., 2013) and is suitable for our study.

Our case organization, a central European university (referred to as CEPU) offers a great setting for observing and analyzing user behavior, as it is a relatively homogeneous, young user group with a high level of education and a high affinity for the internet. CEPU has about 12,000 students and 1,600 employees and is comparable to a large company in terms of organizational complexity. Unlike a commercial enterprise, the university as an educational institution, must act very openly and transparently in its processes, for example to ensure free access to teaching content. CEPU is nevertheless confronted with the same user behavior problems as many other organizations are.

To find out why user behavior often fails to meet security standards, we relied on a qualitative approach conducting semi-structured interviews with different organizational member groups at the CEPU. The three main groups were: the management, the IT department, and the users. The management included department heads, the IT department was represented by representatives of the IT services and IT experts at the university, and the users were represented by the two primary user groups of staff and students at the CEPU. A total of 20 organizational members were interviewed. The interviews were pre-structured using an interview guide. These interviews were recorded and subsequently processed by transcriptions, which formed the basis for further investigation.

To analyze our data, we relied on a grounded theory approach (Strauss & Corbin, 1990). The decisive advantage of this method was that own concepts for theory learning can be worked out from the available data (Glaser, 2002). We chose an open coding approach to interpret the data in this work and for the adopted coding process we followed Gioia and colleagues (2013). At the beginning of the coding process, first order concepts with narrow content, such as lack of knowledge, were coded in the data. Next, these numerous first order concepts were accumulated and combined into thematically overarching second order themes. For example, the first order concepts lack of knowledge, basic knowledge, comprehensive knowledge and need for knowledge were aggregated under the second order theme knowledge.

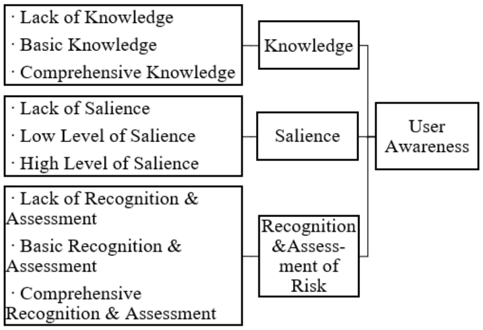
· Lack of Knowledge
· Basic Knowledge
· Comprehensive Knowledge
Knowledge
· Lack of Salience
· Low Level of Salience
· High Level of Salience
Salience
User Awareness
· Lack of Recognition & Assessment
· Basic Recognition & Assessment
· Comprehensive Recognition & Assessment
Recognition &Assess-ment of Risk

Figure 1: Excerpt from data structure.

In a final third step, the second order themes such as knowledge, recognition and assessment of risks and salience were again combined into the superordinate aggregated dimension user awareness (Gioia et al., 2013). Each step was discussed with the team of authors (Gioia et al., 2013). After the data structure was created, the connections between the individual components of the model were established based on the available data. In sum, we derived 5 aggregated dimensions, each consisting of 3 second order concepts. Figure 1 illustrates one aggregated dimension as an example.

4. Findings

User awareness: User awareness consists of three core components: Knowledge, salience, and recognition and evaluation of risks. Knowledge describes the user's level of understanding cyber security related issues. Users themselves often described their own knowledge as basic, but still incomplete: *"Well, I think I already have basic knowledge, especially user knowledge. What I don't know at all [are] simply all the background processes"* (B13, user). During the interviews, users revealed considerable knowledge gaps on the basics of cyber security, which they did not see as problematic: *"I mean, I'm not an IT person either. So, as I said, I don't care either, the main thing is that it works, just like a car."* One user puts it in a nutshell: *"We grew up with the internet [...], but I don't really know anything about it"* (B18, user). Respondents from the IT-department emphasized the need for users to extend their security relevant knowledge as it is an essential part of awareness: *"We might need users to know a bit more and be a bit more knowledgeable, because if you want to drive a car, you also need a driving license"* (B7, IT manager). Additionally, they emphasized the need for a basic understanding of threats and protective measures to protect themselves and the organization: *“You must have a certain expertise in order to be able to create security at all. This also applies [...] to the user because I cannot create security out of ignorance”* (B2, IT manager). One user stressed how important knowledge is for awareness: *“[...] more knowledge would also lead to more recognition, i.e. more awareness“ (*B14, user).

Salience, as another component of user awareness, describes how present the user's relevant knowledge is in their conscious thinking. Some of the interviewed users, especially people with a higher level of knowledge, describe that they subconsciously think about safe behavior when using digital services in organizational networks: *"Well, I don't really actively think about it, but subconsciously I do a bit"* (B14, user). One user mentioned, that salience depends on real-world experience with cyber security issues: *"I think it's primarily a matter of, once you're confronted with it, you're definitely more aware of it"* (B13, user).

Some respondents indicated how important knowledge and salience are for the evaluation and recognition of risks. Whereas, users with little knowledge assessed risks low but admitted their knowledge deficits: *“I think it's like that, that people also underestimate it. So, I think, for me personally, I feel safe. [...] But I also have no idea, as I said, how it works”* (B18, user). Respondents with advanced knowledge and salience appeared to be more capable in the recognizing and assessing of cyber security risks: *“[...] I think the biggest loopholes are probably found in private individuals who are careless at work and click somewhere where they shouldn’t”* (B9, user). Overall, the interviewed users agreed that the majority of users are not sufficiently aware of cyber security issues: *“I think that very few people are aware of the actual consequences of a leak somewhere”* (B13, user).

User IT capabilities: Next, we address the user IT capabilities. In this regard, one user described feeling overwhelmed by threatening situations due to a lack of knowledge on how to react: *“You're really overwhelmed, but I would say that know-how or knowledge [...] is probably what's missing”* (B18, user).

Inexperience with incidents or cyber-attacks plays a crucial role in this context as it impacts the capability to realistically assess potential risks: *“If you've never been confronted with it before, you don't see it as a real danger”* (B13, user). The users in the study showed a very heterogeneous picture of previous experience and stated either that they had little to no experience: *“I have not yet experienced such attacks [...]”* (B1, user) or emphasized their long-standing experience with cyber threats: *“[...] when you have experienced it for years, you are alarmed anyway [...]”* (B6, user), *“In any case, I have often experienced something like that”* (B9, user).

Further, actual know-how is an important component to consider. Many users described their little know-how on cyber security issues: *“On the whole [...] I also have no idea how it works, as I said, but I use it anyway. And I do think that the know-how is lacking a bit”* (B18, user). Users described that they had hardly any experience with cyber-attacks in their everyday life, hindering the development of know-how: *“[I have been] limitedly [confronted] [...] I don't know what I could do to increase security or how”* (B4, user).

Based on experience and know-how, users assessed their actions in terms of cyber security. Inexperienced users often perceived no problems or uncertainties in in this regard: *“I can't think of anything more to do yet, that's why I think it´s fine the way it is”* (B16, user).

Internalization of responsibility: Based on our analysis, we conceptualized internalization of responsibility as interplay of three subdimensions. One such subdimension is externally imposed responsibility, i.e., the perceived level of responsibility that is externally assigned and communicated to users in their role. One user stated it as: *"So I think that responsibility is a bit of a prerequisite, that you already say [...] now at the university, everyone who studies something here or is on the portal should actually already have knowledge about what could happen”* (B17, user).

Some of the respondents stressed that they did not feel that any responsibility was expected from them on the part of the university:

"In my opinion, since I have been enrolled here, the university has never shown any interest in what I do on the internet, or [...] pointed out that the university is a potential target and that we should please deal with it ourselves or support it so that it doesn't become a problem." (B10, user)

Some of the interviewees pointed out the different roles of staff and students across roles at the university. For example, they described the external responsibilities for staff as far more extensive than for students:

"As a rule, all universities have IT regulations that oblige users [...] to report an IT incident [...]. I see that especially for employees, that they have the duty to do so. [...] And whenever students take over functions at the university, student representatives and the like, then the same applies to them as it does to employees." (B11, IT manager)

In this context, one user describes that he considers the responsibility of employees to be high: *"I think that employees are then also more [responsible] in the context, because you don't want to somehow reveal emails or something. [...] But I do think that we have a certain responsibility"* (B18, user). Especially users who are active as both students and employees described strong differences between the imposed external responsibility in the work context vs. the student context. Training and safety requirements from the work context were given as a main reason:

"The responsibility is simply enormous in working life and accordingly you have to be much more careful. And perhaps as a note, we all had to take a training course about IT security. How do I recognize fake links? How can I tell if something I'm looking at is serious or not? And so on" (B15, user).

The communication of responsibility by the organization can be crucial to internalize the responsibility for one's own cyber security behavior: *"I think it is an important point. So, you also have to convey to people that it is the responsibility of each individual either to deal with it or to do something about it."* (B15, user).

Further, the distribution of responsibility plays an important role. This describes the perceived distribution of responsibility between the IT department or the IT managers in the organization and the users. Some of the users interviewed attribute a high degree of responsibility to the IT managers and refused to take some responsibility on themselves: *"No. Well, I don't have the feeling that I should do anything about it. I rather feel that the university has to ensure that we are all safe on the platforms, yes"* (B4, user). Other users and IT managers however emphasized the shared responsibility between IT and users: *"People need to know what they are doing when they handle critical data and you also need to create technical frameworks so that you can intercept accidents, you need to do both"* (B7, IT manager) and: *"I see it as my responsibility to handle these emails responsibly and not to click on any links. But yes, I would also see the university as being responsible for informing students about what to do with such emails [...]"* (B5, user).

Finally, there is internally perceived responsibility. It describes the personally perceived degree of responsibility that the user feels for his or her own actions. Few of the users interviewed expressed a concrete sense of responsibility for their own actions:

"If you reflect on it more, then you are definitely responsible for it. You are probably just not always so aware of it [...]" or: *"Yes, I think so [that I am responsible]. So just in terms of phishing emails, both as a student and as a staff member. So, I think so because a leak somewhere is also a leak somewhere for everyone"* (B13, user).

Users who showed a higher level of knowledge and know-how in advance felt responsible for their own behavior: *"I [would] already say, yes, that my own behavior is of course also important"* (B14, user). On the other hand, users with particularly little knowledge and experience described themselves as not responsible for cyber security.

User behavior: One pillar of organizational cyber security is user behavior. Based on our analysis, desirable user behavior regarding cyber security depends on three subdimensions. One subdimension is the acceptance of security measures, i.e., the acceptance of technical measures introduced by the IT-department to ensure security, such as regular password changes or spam filters. These may occasionally restrict the work of users but are accepted to fulfil the overriding purpose of security in the company. Most users described this kind of behavior as their standard protection procedures: *"I think you need to change your password every 90 days, maybe [you could] possibly [protect] it even more with double authentication"* (B16, user). However, some of the users also described inadequacies in their own user behavior:

"I'm not as sensitive with my password for the portal and so on as I am with my access data for online banking, which is of course also accessed in every public WLAN. [...] Personally, I could handle it more responsibly. I just don't do it. But I could do it." (B17, user)

Further, IT-compliant behavior by users, i.e., actions that are in line with the policies and guidelines of IT to secure organizational IT. This includes, for example, the use of antivirus programs or adequate behavior in dealing with phishing emails. One user describes her own user behavior regarding phishing emails as follows:

“When I get an email like that, I first check for sure whether it's really something that could affect me, and I think even if it looks as authentic as it is and comes across as realistic, if it has even the slightest appearance, I would ask first before I click on anything.” (B6, user)

Some users stressed how compliant behavior benefits all parties involved: *"Just have a virus program on the computer [...]. Exactly as I said, simply promoting one's own security and thereby contributing to the common good”* (B16, user).

Another subdimension is user's active contribution to cyber security, which manifests, for example, in reporting suspicious emails or actions or informing other users about possible or acute dangers. One user explains this with an example of how she acted in relation to phishing emails: *“The first time I got something like that from my boss, I also forwarded it to him and said, I guess you can't do anything, but just that you know about it [...]”* (B6, user). When asked how they could improve their own user behavior in the future, some users described that they could be more active: *"Well, I think you could maybe report more if you really get a phishing email like that”* (B13, user).

Organizational IT: The second pillar of organizational cyber security is the organizational IT, which includes all IT structures and processes relevant to cyber security within the company. In the interviews the central components of cyber security infrastructure, cyber security responsibility, and cyber security strategy were addressed. IT managers explained the parts in the infrastructure that are most frequently attacked:

“Well, everything that is publicly visible, such as websites, services that are often used by students. [...] Otherwise, it's essentially quite banal things, namely phishing attacks. That is the main target, parallel to these real attacks on technical systems, are simply the soft things, phishing, then sometimes threatening emails.” (B2, IT manager)

Further, there is the cyber security strategy. Here we refer to planning and managing security of activities focused at the IT interactions of users in an organization. This includes information, communication, and user support. One interviewee described that users contact the support especially when they are unsure how to deal with cyber risks.: *“I mean, there are also some requests: ´I have an email, I don't trust myself to open it´, so [...] advice and services are also desired”* (B3, IT manager).

Regarding cyber security information and dangers, one user described his positive experience:

“If I remember, this also happened recently, for example, via this update, that there was something in it that there are more phishing mails. [...] So, as I said, I found it quite positive when it was pointed out in this one update.” (B5, user)

However, many users criticized the lack of information and training in cyber security issues:

“[...] and at least at the university I've never come across them warning you about it or telling you how to deal with it if you get an email like that. I don't think the university prepares you for it or informs you about it.” (B1, user)

It became very clear in the interviews that many users would like more information and support from the CEPU. Many of the interviewees emphasized how positively they would perceive additional information and support services at the university: *“So maybe it would be a cool thing if you didn't necessarily do a training course, but somehow a workshop or an event where people talked about the topic. Because I personally don't know anything about it [...]”* (B4, user). In addition, one user points out that a collective warning could be distributed to all members of the university via the regular notification system, especially in the case of frequent phishing attempts: *“If you get an update every Wednesday, then you have to point out that there is already a big problem or that it could become a problem if we don't behave securely [...]”* (B10, user).

The last important component of organizational IT is cyber security responsibility. This subdimension is concerned with accountability for cyber security in an organization. Users subscribed the responsibility for communication of security relevant information to the IT department and emphasized the need for a better information policy: *"But for the students, for example, I would like to see something where they are made a little more aware of how to deal with it correctly”* (B15, user). In addition, many of the users described that they would like to see more offers such as workshops. However, they also acknowledged their own responsibility to take such offers: *"But nevertheless, it would certainly not be bad to perhaps also approach the students and if there are also offers, to then also accept them."* (B15, user). Respondents further stated that they would generally like the IT department to work more closely with the users and to improve communication and exchange: *"From that point of view, I would really like the university to take a step towards the students, perhaps even towards its own employees."* (B15, user). Regarding to the threat reporting, users expected the IT department to provide a simple procedure for reporting security incidents, helping users to adapt their behavior:

"[...] maybe just simplify the whole thing a bit, so that I don't have to go to the website and then search for a thousand subcategories and pages for the contact form again, but just provide a simple email address I can write to" (B13, user).

5. Model development

Figure 2 shows the resulting model we derived from literature combined with the findings of our qualitative study. As is standard for inductive qualitative research, we engaged in a cycling process to repeatedly compare our findings from the interviews with existing literature and developed our model based on both (Gioia et al., 2013). Especially, user awareness (e.g., Bulgurcu et al., 2010), IT capabilities (e.g., Ani et al., 2019), and responsibility (e.g., Siponen, 2000) were previously discussed factors in our research context. As they further repeatedly emerged as topics in our early interviews, we explicitly asked our interviewees for these factors' natures. Further, following the notion of cyber security as socio-technical phenomenon (e.g., Acuna et al., 2021), we expected to see a human (i.e., behavior) and a technical (i.e., IT) component to cyber security, which also became apparent through the interviews. Users and IT managers frequently addressed these two sides of the same coin, as shown in our results. The model, we eventually derived on this twofold basis, provides a comprehensive overview of the interrelations between the different components of organizational cyber security, especially focusing on desirable user behavior.

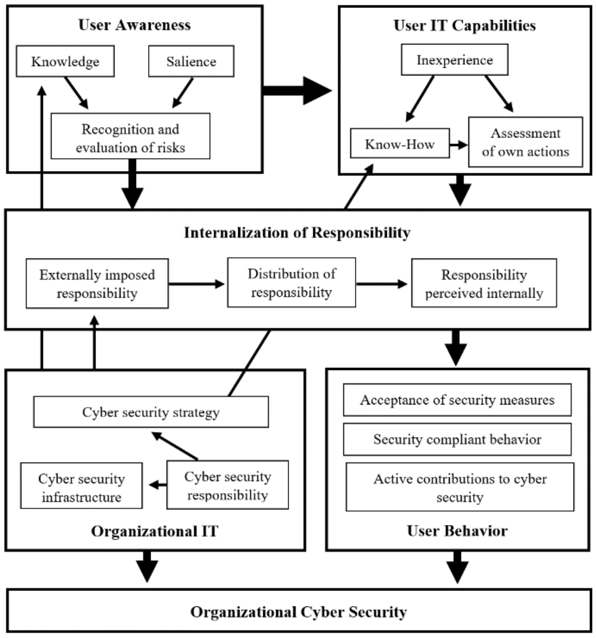
User Awareness
Knowledge
Salience
Recognition and evaluation of risks
User IT Capabilities
Inexperience
Know-How
Assessment of own actions
Internalization of Responsibility
Externally imposed responsibility
Distribution of responsibility
Responsibility perceived internally
Cyber security strategy
Cyber security infrastructure
Cyber security responsibility
Organizational IT
Acceptance of security measures
Security compliant behavior
Active contributions to cyber security
User Behavior
Organizational Cyber Security

Figure 2: Model for managing organizational cyber security.

User awareness: Knowledge, salience, and the resulting benefits for the recognition and evaluation of cyber security risks, defines user awareness in our model. The user's general and specific knowledge about cyber security risks and counteractive security measures (Bulgurcu et al., 2010; Culnan et al., 2008; Dinev & Hu, 2007; Pahnila et al., 2007; Parsons et al., 2014) offers a solid basis for users to recognize and evaluate risks accurately. However, we argue, that knowledge alone does not suffice. The knowledge must also be salient. Here, salience describes how present relevant knowledge is in the users' conscious thinking. Only when the users' knowledge on cyber security issues is salient, they can make sense of that knowledge at the right time. Salience thereby improves recognition and assessment of risks, because users act and think cautiously in everyday IS interactions as they become more sensitive to small anomalies. A potential way to strengthen users' salience is to directly confront them regularly with cyber security issues and to draw their attention to them (e.g., through regular workshops). Recognition and evaluation of risks supports the internalization of responsibility. This was also illustrated by our data, as respondents who were aware of potential risks, frequently stated that they perceived responsibility for the organizations cyber security.

IT capabilities: The users' IT capabilities (i.e., the user's abilities to respond adequately to threats or incidents) are a crucial component of cyber security (Ani et al., 2019; Workman et al., 2008). Our data indicated, that capabilities are supported by user awareness, as knowledge about cyber security risks and potential countermeasures builds the basis for avoiding such risks and applying appropriate countermeasures in case of cyber security incidents. Besides awareness, inexperience and know-how play a major role for IT capabilities. Inexperienced users cannot base their actions on comparable situations from the past. Further, inexperience is negatively related to know-how. Here, know-how describes the users' abilities to react appropriately to an incident. Know-how can only be built through undergoing similar real-world situations or hands-on training. With little experience and know-how, users run the risk of misjudging their own actions., which further hinders the development of capabilities. Our analysis showed that inexperienced users tended to assesses their own actions (too) favorable and thus, in some cases, perceive no need to improve their IT capabilities. However, IT capabilities are crucial, as they also have a positive influence on the internalization of responsibility. They reduce risky behavior and enable a more accurate assessment of one's own actions. Thereby, they strengthen the willingness to take responsibility for one's own actions.

Internalization of responsibility: We conceptualize the internalization of responsibility as degree, to which users feel responsible for their behavior and the resulting outcomes when using organizational IT (de Bruijn & Janssen, 2017; Filipczuk et al., 2019; Siponen, 2000). This means, that users not only recognize risks, evaluate them and react to them, but also feel responsible for displaying a certain behavior. This component is shaped by three subdimensions: First, there is externally imposed responsibility, which is the perceived level of responsibility that is externally assigned and communicated to users in their organizational role. Further, there is the distribution of responsibility, which is the assumed distribution of responsibility between the organization (i.e., IT department/IT managers) and the users (i.e., the degree of responsibility users assume to apply to them). The more responsibility is imposed on users externally (e.g., through measures that deter undesired or reward desired behavior), the more responsibility they assume for themselves. Last, there is responsibility perceived internally, i.e., the degree of responsibility that users feel for their own actions. Internally perceived responsibility is related to the distribution of responsibility. The more responsibility users assume they must take on compared to the organization, the more they will internalize responsibility for themselves. We argue, that internalization of responsibility is positively related to desirable user behavior.

User behavior: Cyber security behavior in organizations includes actions and avoidance in relation to organizational cyber security measures. Due to the socio-technical nature of cyber security, user behavior plays a central role for organizational cyber security (Corradini & Nardelli, 2018; Culnan et al., 2008; de Bruijn & Janssen, 2017; Sankaranarayanan et al., 2007). From the data, we derived three relevant subdimensions for desirable user behavior in the given context. First, there is the acceptance and adherence of security measures, i.e., technical measures introduced by the IT-department to ensure security, such as regular password changes or spam filters. Second, compliant user IT behavior such as actions that are in line with the policies and cyber security guidelines of the organization is vital. This includes, for example, the use of antivirus programs or adequate behavior in dealing with phishing emails. Finally, there is user's active contribution to IT security, including for instance the reporting of suspicious incidents. These three subdimension of desirable user behavior can be seen as three levels that emerge as users gain knowledge and experience. The acceptance of security measures is a rather passive support of the organization’s cybersecurity strategy, while IT-compliant behavior and especially active contributions to IT security represent active support of the organizational cyber security by the users.

Organizational IT: Here, we refer to the part of an organization’s IT environment, that is related to cyber security. In particular we focus on parts that can impact desirable user behavior, i.e., the cyber security infrastructure, the responsibility for cyber security in an organization, and the organizational cyber security strategy. Responsibility, i.e., the overall responsibility for a secure organizational IT environment, usually is with the IT department. This responsibility requires to design and maintain the IT infrastructure in a way that ensures its security of soft- and hardware. Further, this responsibility entails developing and updating a cyber security strategy comprising measures that can directly affect user awareness, user IT capabilities, and the internalization of responsibility. In particular, our interviews revealed that communicating frequently attacked parts of the IT infrastructure and the kinds of attacks raises users’ awareness and offers a base for improving IT capabilities (e.g., recognizing phishing mails). The cyber security strategy can also determine the extent to which cyber security trainings are offered to improve IT capabilities. Further, it directly contributes to the internalization of responsibility by determining the degree of distribution of responsibility and by externally imposing responsibility through active communication, highlighting sanctions and rewards for non-compliant and compliant behavior respectively.

6. Discussion

6.1. Implications for research and practice

For research, our study offers two major implications on organizational cyber security. First, by enriching fragmented literature with findings from our qualitative study, we offer an integrated comprehensive model for organizational cyber security management. Based on our qualitative data, we elaborated in detail the interrelations of the components that make up our model (see 5. Model development). Through these elaborated interrelations, we show how desirable user behavior has a central role in the socio-technical context of organizational cyber security and how user awareness, user IT capabilities, and especially internalized responsibility shape behavior in this context. Thereby, we provide new insights related to the ongoing discussion on the understanding of cyber security compliance (Chen et al., 2021; Jenkins et al., 2021) and provide new potential explanations, why users behave in ways that are desirable in terms of cyber security guidelines and policies in organizational contexts.

Second, we show that internalization of responsibility is a key concept for desirable user behavior in cyber security and can be seen as an intermediate stage between user awareness and actual user behavior. With the internalization of responsibility, we incorporated an existing concept into our model (Siponen, 2000), which we extended by the perceived distribution of responsibility. We argue, that this better accounts for the shared responsibilities between organization and users in reality. Further, this highlights the benefits of shared responsibility as in de Bruijn and

Janssen (2017). In line with LaRose and colleagues (2008), the presented results show that a sense of personal responsibility has a positive impact on behavior and benefits compliance to security requirements. However, internalizing responsibility requires user awareness and user IT capabilities. Our results confirm previous findings that in the absence of user awareness or insufficient user IT capabilities, responsibility is not internalized and users thus do not show desirable, i.e., cyber security compliant, behavior (Furnell et al., 2007; LaRose et al., 2008).

For practice, we offer several implications too. We showed that strengthening awareness factors such as the users' knowledge or targeted awareness campaigns have a positive effect (Culnan et al., 2008; Parsons et al., 2014). This improves in the recognition and evaluation of risks, which has a positive effect on the users' internalized responsibility. The study reveals that user education is essential, as many of the respondents described their own knowledge as insufficient and their levels of experience and know-how as low. User- and context-specific workshops and realistic training examples are necessary to improve the users' internalization of responsibility. Further, organizations should clearly communicate expectations regarding the user's responsibility. This increases the responsibility imposed externally and give the users feelings of actually being responsible for their behavior. Regular reminders and targeted IT guidelines comprising clear expectations and recommendations can achieve this.

No single measure will lead to success, but a mix of methods involving knowledge transfer, training, continuous support, and an incentive system that relies on rewards and deterrence promises greatest possible effects for organizations. Yet, in order to actively shift user behavior into a desirable direction, it is important to define what exactly desirable behavior entails and how it is measured. In our case, desirable behavior refers to behavior compliant to CEPU's cyber security guidelines, e.g., keeping antivirus programs updated, changing passwords regularly, avoiding suspicious links, and reporting suspicious e-mails. Potential metrics to measure the degree of desired user behavior could comprise the number of incidents caused by human (mis-)behavior, the user share with outdated antivirus programs, the number of cyber security trainings, and number of reported e-mails with suspicious content.

6.2. Limitations and future research

The interviews with members of the CEPU gave us a good first impression of the topic. However, all participants in this study were members of the same organization, limiting variety regarding user and IT manager perspectives. Although, the CEPU is comparable to a company in terms of organizational complexity the processes, IT systems at universities are designed more openly than in a company. In a company, users may also show higher levels of perceived responsibility than students in a university context.

Future research should investigate the internalization of responsibility in more detail. Here, we provided a first step. Yet, we need a deeper elaboration of the concept and a more precise definition of the scope of responsibility that users should assume. Further, it should be investigated in more detail, if there are additional components that have been omitted in this study. External factors such as the environment in which users operate, demographic factors such as age, gender and origin, or sociological factors such as internalized values and norms are conceivable. Finally, it should be noted that the responsibility of users in the context of cyber security in organizations must be given more attention, both in theory and in practice, to bring about sustainable changes in user behavior.

7. References

Acuna, D., Suliman, R., & Elmesmari, N. (2021). A Practitioner Methodology for Mitigating Electronic Data Risk Associated with Human Error. *Journal of the Midwest Association for Information Systems, Vol. 2021*(2), Article 2.

Aggarwal, R., Kryscynski, D., Midha, V., & Singh, H. (2015). Early to Adopt and Early to Discontinue: The Impact of Self-Perceived and Actual IT Knowledge on Technology Use Behaviors of End Users. *Information Systems Research*, *26*(1), 127–144.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2–35.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Proceedings of the International Conference on Cyber Security for Sustainable Society, Coventry*.

Balozian, P., & Leidner, D. (2017). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 48*(3), 11–43.

Bitkom. (2021). *Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr*. https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Braue, D. (2021). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. *Cybercrime Magazine*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523–548.

Chen, Y., Galletta, D. F., Benjamin Lowry, P., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Information Systems Research, 32*(3), 1043–1065.

Corradini, I., & Nardelli, E. (2018). Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. *International Conference on Applied Human Factors and Ergonomics,* 193–202.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21.

Culnan, M. J., Foxman, E. R., & Ray, A. W. (2008). Why IT executives should help employees secure their home computers. *MIS Quarterly Executive, 7*(1), Article 6.

D´Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79–98.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7.

Deloitte. (2021). *Cyber Security: So können Unternehmen sich gegen Attacken schützen*. https://www2.deloitte.com/de/de/pages/risk/articles/Cyber_Security.html

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(7), 386–408.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review, 14*(4), 532–550.

Filipczuk, D., Mason, C., & Snow, S. (2019). Using a Game to Explore Notions of Responsibility for Cyber Security in Organisations. *CHI Conference on Human Factors in Computing Systems*, 1–6.

Furnell, S. M., Phippen, A. D., & Bryant, P. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410–417.

Gioia, D. A., Corley, K. G., & Hamilton, A. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31.

Glaser, B. G. (2002). Conceptualization: On Theory and Theorizing Using Grounded Theory. *International Journal of Qualitative Methods, 1*(2), 23–38.

Herath, T., & Rao, & H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81.

Jenkins, J. L., Durcikova, A., & Nunamaker, J. F. (2021). Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship. *Journal of the Association for Information Systems, 22*(1), 246–272.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., & Jun, C. R. (2021). Cyber Security in the Age of COVID-19 : A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *Computers & Security, 105*, 102248.

LaRose, B. R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71–76.

Macabante, C., Wei, S., & Schuster, D. (2019). Elements of Cyber-Cognitive Situation Awareness in Organizations. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 1624–1628.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151–156.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICCS'07)*, 156–166.

Pan, J., & Yang, Z. (2018). Cybersecurity Challenges and Opportunities in the New ``Edge Computing + IoT'' World. *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 29–32.

Parsons, K. A., McCormac, A., Butavicius, M. A., B., P. M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Sankaranarayanan, V., Chandresekaran, M., & Upadhyaya, M. (2007). Position: The User is the Enemy. *Proceedings of the New Security Paradigms Workshop,* 75–80.

Sen, R. (2018). Challenges to Cybersecurity: *Current State of Affairs. Communications of the Association for Information Systems, 43*(1), 2.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503–522.

Strauss, A., & Corbin, J. (1990). *Basics of grounded theory methods*. Sage.

Von Skarczinski, B. S., Dreissigacker, A., & Teuteberg, F. (2022). More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM. *Wirtschaftsinformatik 2022 Proceedings*.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816.