Shouldering the Shield: The Vital Role of Internalized Responsibility in Managing Organizational Cybersecurity

Kosay Tabaja

Charisma University,
Address of 1st author, Country, PH-001 657 567 5676
kosaytabaja@hotmail.com

Abstract: In today's digital age, cybersecurity has become a top priority for organizations. While many companies invest in the latest security technologies and protocols, they often overlook the importance of internalized responsibility in managing cyber threats. This article explores the vital role that internalized responsibility plays in safeguarding an organization's sensitive information and assets from cyber-attacks. By examining case studies and industry best practices, we showcase how a culture of accountability can foster better cybersecurity hygiene among employees at all levels of an organization. From senior leadership to entry-level staff, everyone must shoulder the shield and take ownership of their role in protecting their company's digital assets. Ultimately, this article argues that internalized responsibility is a critical component of any comprehensive cybersecurity strategy and should be given equal attention alongside technological solutions.

Keywords: accountability, cybersecurity, culture of accountability, cyber threats, cybersecurity strategy, digital assets.

1. Introduction

In today's hyper-connected world, cybersecurity has become a critical concern for organizations of all sizes and industries. As businesses increasingly rely on digital infrastructure to store and manage sensitive information, they face mounting risks from cyber-attacks. The consequences of a breach can be severe, ranging from financial losses to reputational damage and legal liabilities [19].

While many companies invest heavily in the latest security technologies and protocols, they often overlook the importance of internalized responsibility in managing cybersecurity risks. Internalized responsibility refers to a culture of accountability where all employees take ownership of their role in protecting the company's sensitive information and assets from cyber-attacks [16]. This includes everyone from senior leadership to entry-level staff.

The human factor has been identified as the weakest link in cybersecurity [22]. In fact, according to a recent report by IBM Security and Ponemon Institute, over half of all data breaches are caused by human error or system glitches [22]. This highlights the need for organizations to focus not only on technology solutions but also on cultivating a culture of accountability around cybersecurity.

In recent years, there has been growing recognition of the vital role that internalized responsibility plays in managing organizational cybersecurity. By examining case studies and industry best practices, experts have showcased how a culture of accountability can foster better cybersecurity practices among employees at all levels [27]. In fact, NIST emphasizes that internalized responsibility is a critical component of any comprehensive cybersecurity strategy and should be given equal attention alongside technological solutions [27].

Moreover, research suggests that organizations with strong cultures of accountability tend to have fewer data breaches than those without such cultures [5]-[19]-[27]. These findings underscore the importance of internalized responsibility as an effective means for reducing cyber risk.

In conclusion, while technological solutions are important for mitigating cyber risks, it is equally essential for organizations to cultivate a culture of accountability around cybersecurity. Internalized responsibility can help achieve this goal by empowering employees at all levels to take ownership over protecting their organization's digital assets. By doing so, companies can reduce their exposure to cyber threats and build a stronger overall security posture.

2. Research Background

Organizational cybersecurity is an increasingly important issue in today's digital age. Organizations have to respond quickly and effectively to a growing number of threats, ranging from malware attacks to data breaches. In recent years, organizations have been taking steps to strengthen their cyber defenses by utilizing a variety of technologies, such as firewalls and antivirus software, as well as investing in security personnel and training. However, these efforts are only part of the solution; organizations must also be mindful of the role that internalized responsibility plays in ensuring the security of their systems and data. This paper examines the concept of internalized responsibility within an organizational context and how it can contribute to successful cybersecurity management.

2.1. The Role of Internalized Responsibility

Internalized responsibility has been defined by researchers as "the psychological process of taking ownership of one's own actions and decisions, including the consequences that may arise from them." [21]. This concept is closely related to the idea of self-efficacy, which was developed by Bandura [4] to describe an individual's belief in their own ability to complete a task successfully. Internalized responsibility also

involves recognizing and accepting that negative outcomes can occur due to one's actions or decisions, and taking steps to mitigate such risks.

In terms of organizational cybersecurity management, internalized responsibility refers to individuals within an organization taking ownership for protecting their systems and data and not relying solely on external solutions. It involves understanding the implications of any given action or decision, and being aware of the potential negative consequences that may arise from it. Furthermore, individuals must be willing to take responsibility for their actions and be prepared to face any resulting penalties or repercussions.

Studies have shown that internalized responsibility is an important factor in successful cybersecurity management [24]. Organizations that encourage a culture of personal accountability are more likely to succeed in protecting their systems and data from cyberattacks. This can be achieved through various measures, such as providing employees with training on how to recognize potential threats and respond appropriately, as well as fostering a sense of collective ownership for the organization's security posture.

2.2. Organizational users and cyber security

Consistent with existing Information Systems (IS) - research, we view cyber security as a sociotechnical phenomenon [1]-[9]-[10]; in the sense that neither a purely technological nor a purely human-centered perspective can adequately explain the phenomenon. However, we concur with IS-scholars who emphasize the unique role of users and their behavior in relation to cyber security [8]-[10]-[12], arguing that even the security of systems protected by highly sophisticated technical measures is dependent on how users use these systems. In contrast to software and hardware, users cannot be thoroughly monitored for legal, ethical, and technical reasons, nor can they be easily upgraded, when possible, security problems are identified. This hinders the detection and prevention of cyber security breaches resulting from user misconception, misconduct, or inattention. Users are, thus, a weak link in the cyber security metaphorical chain [8]-[12]-[32]. Consequently, practitioners and experts are placing a greater emphasis on training and development to modify user behavior and ultimately enhance cyber security [6]-[10]-[12]-[30]. In conclusion, cyber security IS literature emphasizes the significance of user behavior.

In addition to the fundamental role of the user, the literature emphasizes the significance of the various contexts in which cyber security research is conducted [3]. The emphasis of this study is an organizational context. Organizational settings are commonly the subject of cyber security research by academics [3]- [10]-[15]-[26]. This context is characterized by a formal interaction between an organization and its IT-using workers. Users have rights and responsibilities for the use of corporate IT, and both parties are involved in the development and implementation of a cyber security strategy. It is possible for context elements to vary between companies or types of organizations. Depending on an organization's size, industry, or mission, the available cyber security management resources (e.g., cyber security-training and education, mechanisms to discourage undesirable user behavior and to promote acceptable conduct) vary [1].

2.3. Organizational cyber security management

Awareness is the component most usually mentioned in relation to cyber security management. Awareness is dependent on the user's general and specific knowledge of cyber threats and countermeasures[6]-[10]-[13]-[28]. To be able to behave in a manner that prioritizes security, the user must first have a comprehensive understanding of the operating environment. Hence, numerous studies advocates enhancing user knowledge through focused education and training initiatives [3]-[28]. Knowledge expansion can preventatively ensure that consumers are more aware of potential threats at an earlier stage and are therefore better educated beforehand [3]. Yet, Aggarwal and colleagues (2015) note that users' self-assessed and actual cyber security expertise frequently diverge significantly. This frequently results in consumers overestimating their own abilities and failing to actively seek out new information.

In addition to knowledge, the computer skills of users are a critical component of corporate cyber security management [1]-[33]. Users cannot actively assist organizational cyber security if they are unable to appropriately respond to dangerous events. To enhance these capacities, tailored training of users' practical knowledge is required to equip them with understanding of applicable procedures for preventing or responding to dangerous situations [3].

In addition to awareness and IT capabilities, the literature frequently addresses responsibility. [29] coined the term prescriptive awareness to describe a combination of role and moral responsibility. This involves taking responsibility for one's own digital activity and displaying safe conduct, such as implementing security measures[13]. In order to encourage such ideal user behavior, IT managers can impose external responsibility on users. In this regard, measures to influence users' motivation play a central role [20], primarily consisting of measures to deter undesirable, security non-compliant behavior through sanctions such as reprimands [11] and measures to reward desired behavior, such as through monetary rewards. Hence, deterrence tactics try to increase the cost of noncompliance, making it less appealing to individuals, while rewards aim to increase the advantages of complying behavior, making it more appealing [6]. In addition, based on the findings of their study, [12] urge for shared accountability between users and higher hierarchical levels, emphasizing that shared responsibility for cyber security results in improved implementation of digital security measures. [25] demonstrate that users who viewed safe behavior as their personal responsibility were substantially more compliant than users who did not view safe behavior as their personal responsibility. Users tasked with a high level of responsibility for their own digital activity readily accepted it and followed security standards, as confirmed by [15]. Both studies shows that individual accountability plays an essential role in enhancing user behavior.

Although the aforementioned components are extensively described in the literature, their interrelationships, impact on user behavior, and integration into a comprehensive model for organizational cyber security management are absent. To

address this gap in existing research, we conducted a qualitative case-based study in which we asked participants about these interrelationships.

3. Methodology

We did a qualitative case study to acquire insight into the interrelationships and connections between the various components of corporate cyber security management and ideal user behavior. This strategy permits the observation and comprehension of underlying mechanisms and relationships and is appropriate for our study [14]-[17].

Our case organization, a university in central Europe (CEPU), provides an ideal environment for observing and studying user behavior, as its user population is reasonably homogeneous, youthful, and highly educated, with a strong passion for the Internet. CEPU has around 12,000 students and 1,600 personnel, and its organizational complexity is equal to that of a large firm. In contrast to a commercial firm, the university, as an educational institution, must behave very publicly and honestly in its operations, such as by ensuring free access to instructional materials. Despite this, CEPU faces the same user behavior issues as several other organizations.

To determine why user behavior frequently fails to comply with security criteria, we employed a qualitative strategy consisting of semi-structured interviews with several organizational member groups at the CEPU. Management, the IT department, and the users were the three primary groups. The administration consisted of department heads, the IT department was represented by representatives of the university's IT services and IT professionals, and the users were represented by the two key user groups at the CEPU: employees and students. Twenty members of the organization were questioned in all. An interview guide was used to pre-structure the interviews. These interviews were taped and then transcribed, which served as the foundation for additional inquiry.

To analyze our data, we employed a grounded theory methodology [31]. Own conceptions for theory learning could be derived from accessible facts, which was the major advantage of this strategy [18]. We used an open coding strategy to understand the data in this study, and we followed Gioia' coding methodology (2013). First order concepts with narrow content, such as lack of understanding, were recorded in the data at the beginning of the coding process. Then, these multiple first-order notions were compiled and merged into thematically encompassing second-order themes. For instance, the first order ideas absence of knowledge, fundamental knowledge, comprehensive knowledge, and the need for knowledge were grouped under the second order theme knowledge.

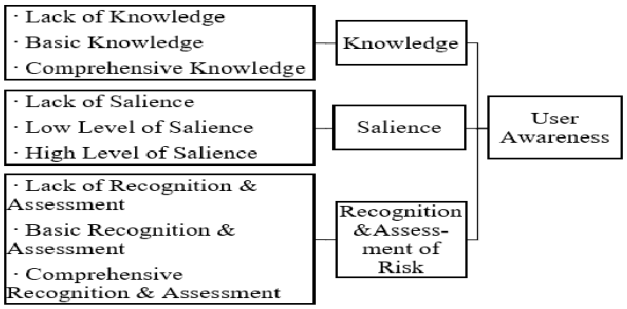

Figure 1: Excerpt from data structure

In a third and final step, second-order themes such as knowledge, recognition and assessment of dangers, and salience were once more merged into the superordinate aggregated dimension user awareness [17]. Each stage was reviewed with the author group. Using the provided data, the linkages between the model's separate components were formed after the data structure was created. In total, we produced five aggregated dimensions, each of which comprised three second-order ideas. Figure 1 depicts an example of an aggregated dimension.

4. Findings

User awareness consists of three fundamental components: knowledge, salience, and risk recognition and appraisal. Knowledge represents the user's level of cyber security-related comprehension. People frequently described their own expertise as elementary but nonetheless insufficient: "*I believe I already possess fundamental knowledge, particularly user knowledge. What I am completely unaware of are the background processes* " (B13, user). During interviews, consumers exhibited significant knowledge gaps regarding cyber security fundamentals, which they did not view as worrisome "*I am not an IT professional either. As I already stated, I too do not care as long as it functions, much like a car." In the words of one user, "We grew up with the internet [...] yet I don't actually know anything about it*" (B18, user). Respondents from the IT-department emphasized the need for users to increase their security-related knowledge, as it is a crucial aspect of awareness: "*We may need users to know a little bit more and be a little bit more knowledgeable, because if you want to drive a car, you also need a driver's license*" (B7, IT manager). In addition, they underlined the necessity for a fundamental awareness of dangers and preventive measures to safeguard themselves and the organization: "*In order to build security at all, you must have a certain level of expertise. This also applies to the user, as I cannot construct security from ignorance*" (B2, IT manager). One user emphasized the significance of information for awareness, stating, *"[...] more knowledge would also lead to more recognition, i.e. more awareness*" (B14, user).

As a component of user awareness, salience reflects how present the user's pertinent knowledge is in their conscious thought. Several of the interviewed users, particularly those with a greater degree of understanding, report that they subconsciously consider safe behavior when using digital services in corporate networks (B14, user). One user stated that salience is determined by real-world exposure to cyber security issues: "*I believe it's mostly a matter of once you're confronted with it, you're obviously more conscious of it*" (B13, user).

Some respondents emphasized the significance of knowledge and salience in assessing and recognizing dangers. In contrast, individuals with less information rated hazards as low but acknowledged their ignorance: "*I believe that this is the case, that people tend to underestimate it. So, I believe I personally feel secure. [...] Yet, I also have no understanding how it operates*" (B18, user). Individuals with extensive knowledge and salience appeared to be more adept of spotting and analyzing cyber security hazards. *"[...] I believe the largest security gaps are probably located in irresponsible employees who click on inappropriate websites*." (B9, user). Overall, the interviewed users concurred that the majority of users lack appropriate cyber security awareness: "*I believe that very few individuals are aware of the actual repercussions of a breach someplace*." (B13, user).

User IT capabilities: Next, the user IT capabilities are addressed. In this regard, one user reported feeling overwhelmed by frightening events owing to a lack of understanding on how to respond: "*You're extremely overwhelmed, but I would say that knowledge [...] is probably what's missing*." (B18, user).

"*If you've never been presented with it before, you don't view it as a real threat*," (B13, user). The users in the survey painted a very diverse picture of their prior experience, with many claiming to have little or none: "*I have not yet encountered such attacks*." (B1, user) or stressed their lengthy exposure to cyber threats: *"[...] when you have experienced it for years, you are still frightened [...]*" In any case, I have frequently seen similar situations. (B9, user).

In addition, actual expertise is a crucial consideration. Several users acknowledged their little cyber security knowledge as follows: "*In general [...] I have no understanding how it works, but I use it anyhow*." And I do believe that the expertise is rather inadequate" (B18, user). *"[I have been] limitedly [confronted] [...] I don't know how to boost security or what I could do to do so*" (B4, user).

Users evaluated their behaviors in terms of cyber security based on their expertise and knowledge. Frequently, inexperienced users could not see any issues or uncertainties in this regard: "*I can't think of anything more to change, so I guess it's perfect as is*." (B16, user).

On the basis of our investigation, we framed internalization of responsibility as an interaction between three subdimensions. One such subdimension is externally imposed responsibility, or the perceived level of externally assigned and conveyed responsibility to users in their role. One user said it as follows: "*Therefore I believe that accountability is somewhat of a prerequisite, that you already state [...] now at the university, everyone who learns something here or is on the portal should actually already be aware of what could occur*" (B17, user).

Some of the responders emphasized that they did not believe the institution anticipated any responsibility from them:

"*While I have been a student at this institution, the university has never showed any interest in what I do on the internet, nor has anybody ever mentioned that the university is a potential target and that we should deal with it ourselves or assist it so that it does not become an issue*." (B10, user)

Some of the interviewees highlighted the various roles that employees and students play at the university. For instance, they described the external duties of staff as being considerably greater than those of students:

" *Typically, all colleges have IT policies that require users to report IT incidents. I believe that employees, in particular, have the responsibility to do so. […] And anytime students assume university functions, such as student representatives and the like, the same rules apply to them as to employees*." (B11, IT manager)

In this context, one user states that he believes employee accountability to be significant: " *I believe that employees are then also more [responsible] in this situation, given that you don't want to disclose emails or something. [...] Nonetheless, I do believe that we have some responsibilities*" (B18, user). Particularly users who are both students and employers described significant discrepancies between the external responsibilities imposed in the work context and the school context. The training and security requirements of the workplace were cited as the primary factor:

"*At the workplace, the duty is just enormous, and correspondingly, you must be much more cautious. And possibly as a footnote, we were all required to complete an IT security training course. How can I identify phony links? How can I determine whether something I'm viewing is serious or not? And so forth*" (B15, user).

The organization's communication of duty might be vital to the internalization of cyber security responsibilities: "*I believe it is an essential point. Hence, you must also explain to them that it is their job to either deal with the issue or take action*." (B15, user).

Therefore, the distribution of responsibilities is crucial. This outlines the perceived duty distribution between the IT department or IT managers in the firm and the users. Some of the interviewed users attributed a great deal of responsibility to the IT management and refused to accept any accountability for their own actions: "*No. In any case, I do not believe action is necessary. Yes, I do believe that the institution must assure our safety on the platforms*." (B4, user). Yet, other users and IT administrators stressed the shared duty between IT and users: "*People must understand what they are doing when handling sensitive data, and you must develop technical frameworks to prevent mishaps; you must do both.*" (B7, IT manager) and: "*I consider it my duty to handle these emails appropriately and avoid clicking any links. Yet I would also consider the university responsible for informing students how to handle such communications [...]*" (B5, user).

Lastly, there is an internal sense of responsibility. It represents the user's perceived level of personal responsibility for his or her own activities. Few of the questioned users had a strong sense of personal accountability:

"*With further consideration, you are undoubtedly accountable for it. You are likely not always so conscious of it [...]*" or: " *Absolutely, I believe that I am accountable. Regarding phishing emails, both as a student and as a member of staff, care must be taken. So, I believe that a leak somewhere is a leak somewhere for everyone.* " (B13, user).

Users who demonstrated greater knowledge and expertise in advance felt accountable for their actions: " *Indeed, I would already agree that my personal behavior is obviously also crucial*." (B14, user). Those with limited knowledge and expertise, on the other hand, described themselves as not responsible for cyber security.

User behavior: User behavior is a pillar of corporate cyber security. According to our investigation, the optimal cyber security behavior of users depends on three subdimensions. One subdimension is the acceptance of security measures, or the acceptability of technological measures implemented by the IT-department to ensure security, such as regular password changes and spam filters. They may occasionally restrict the work of users, but they are permitted because they serve the company's paramount security aim. The majority of users described this as their standard security measures: "*I believe you should update your password every 90 days, and you might possibly increase its security with two-factor authentication*." (B16, user). Yet, a few of the users noted deficiencies in their own user behavior:

" *My portal and other passwords are not as critical as my online banking login information, which is of course accessible in every public WLAN. [...] I could personally manage it more responsibly. I just don't do it. But, I could do it.*" (B17, user)

In addition, IT-compliant user behavior, i.e., behaviors that are in accordance with IT regulations and norms, helps to secure the IT infrastructure of a business. This involves the usage of antivirus software and appropriate behavior when dealing with phishing communications, for example. One user expresses her own conduct towards phishing emails in the following manner:

"*When I receive such an email, I first determine if it's truly something that could affect me. If it has even the slightest appearance of being a scam, I would ask first before clicking on any links*." (B6, user)

Some users emphasized how all parties profit from compliance behavior: " *Just install a virus protection application [...]. As stated, only promoting one's personal security and contributing to the greater good is sufficient*." (B16, user).

A further subdimension is the user's active contribution to cyber security, which manifests itself, for instance, in the form of reporting suspicious emails or actions or notifying other users of potential or imminent hazards. This is illustrated through the actions of one user in response to phishing emails: "*The first time I received such an email from my employer, I also forwarded it to him and stated, "I suppose you can't do anything about it, but just so you're aware of it [...]*" (B6, user). When asked how they could enhance their own future user behavior, several users said they could be more active: " *Now, if you truly receive a phishing email like that, I believe you could report it more*." (B13, user).

Organizational IT: The second pillar of corporate cyber security is the IT infrastructure, which encompasses all important IT structures and procedures within the firm. The interviews addressed the essential components of cyber security infrastructure, cyber security responsibility, and cyber security strategy. IT administrators described the infrastructure components that are most commonly targeted:

"*Everything that is publicly accessible, such as websites and services often utilized by students. [...] Otherwise, it is mostly mundane things, such as phishing scams. Parallel to these actual attacks on technical systems, the primary objective is simply the soft things, phishing, and sometimes threatening emails*." (B2, IT manager)

In addition, there is cyber security plan. Here, we refer to the planning and management of security activities centered on the IT interactions of an organization's users. This comprises information, communication, and assistance for the user. One interviewee stated that people typically contact help when they are uncertain how to handle cyber dangers: "*Also, there are some requests: "I have an email, but I don't trust myself to read it," thus guidance and services are also wanted*." (B3, IT manager).

One user highlighted his favorable experience with regard to cyber security knowledge and threats:

"*If I recall correctly, this also occurred recently, for instance via this update, which contained a notification that there are additional phishing emails. [...] As previously stated, I find it pretty encouraging that it was highlighted in this particular release*." (B5, user)

Nonetheless, many users questioned the absence of cyber security knowledge and training:

"[...] At least at my campus, I've never encountered a warning or instructions on how to respond if you receive such an email. I do not believe the university prepares or tells students about it." (B1, user)

Throughout the interviews, it became abundantly evident that a large number of consumers desire additional information and support from the CEPU. Many interviewees stressed how favorably they would see extra university information and support services: "*Hence, it may be good if you didn't necessarily do a training session, but rather a workshop or event where people discussed the topic. Because I know nothing about it directly [...]*" (B4, user). In the case of numerous phishing attempts, one user suggests that a collective warning may be delivered to all university members through the standard notification system: "*If you receive an update every Wednesday, you must indicate that there is already a significant problem or that one could develop if we do not behave safely [...]*." (B10, user).

Cybersecurity responsibility is the final essential element of IT infrastructure. This subdimension addresses cyber security accountability within an organization. Users

entrusted the IT department with the obligation of communicating security-related information and underlined the need for a more effective information policy: " *But for the students, for instance, I would want to see something that would make them a bit more aware of how to handle it correctly*." (B15, user). In addition, some users expressed a desire for more offerings, such as workshops. But they also recognized their obligation to accept such proposals: " *But, it would not be a bad idea to maybe also approach the students, and if there are further offers, to accept them as well*." (B15, user). Respondents also expressed a desire for the IT department to collaborate more closely with users and enhance communication and exchange: " *From this perspective, I would like to see the institution reach out to its students and perhaps even its own workers*." (B15, user). Concerning threat reporting, consumers anticipated that the IT department would provide a straightforward mechanism for reporting security problems, enabling them to modify their behavior:

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

5. Model Development

Figure 2 depicts the model we derived from the literature and the results of our qualitative study. As is typical for inductive qualitative research, we engaged in a cycling process in which we constantly compared our findings from the interviews with existing literature and built our model based on both [17]. In our research environment, user awareness (e.g.,[6]), IT capabilities (e.g., [1]), and responsibility [29] were previously mentioned aspects. As these elements recurred frequently in our early interviews, we directly questioned our interviewees about their natures. In addition, based on the concept of cyber security as a socio-technical phenomenon [1], we anticipated a human (i.e., behavior) and a technical (i.e., IT) component to cyber security, which was also revealed through the interviews. According to our findings, users and IT administrators repeatedly addressed these two sides of the same coin. On the basis of these two considerations, we developed a model that provides a thorough picture of the interrelationships between the many components of organizational cyber security, with a particular emphasis on ideal user behavior.

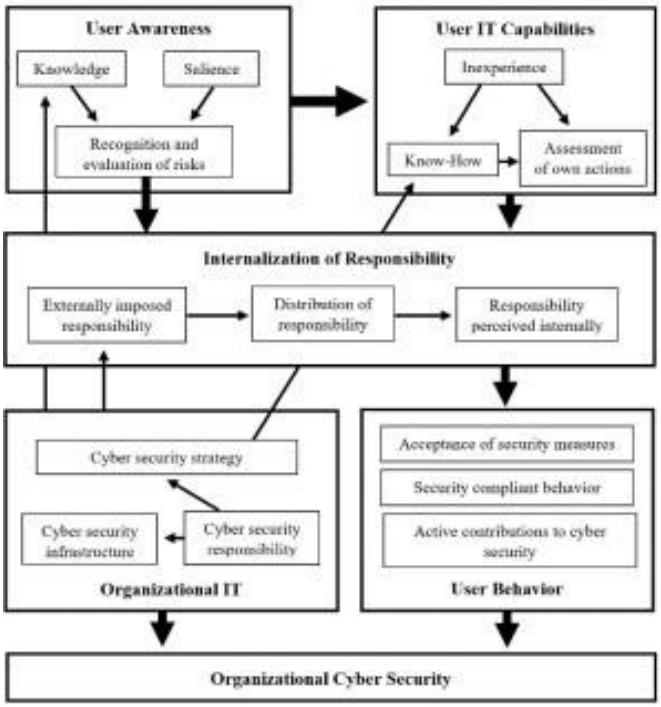

Figure 2: Model for managing organizational cyber security

User awareness: In our model, user awareness is defined by knowledge, salience, and the consequent benefits for the recognition and evaluation of cyber security threats. The user's general and specialized understanding of cyber security risks and countermeasures [6]-[10]-[13]-[28] provides a solid foundation for accurately recognizing and evaluating threats. We contend, however, that knowledge alone is insufficient. Relevant knowledge is also required. In this context, salience reflects how accessible relevant information is to the users' conscious thought. Users can only make sense of their cyber security knowledge at the appropriate moment if their information is pertinent. As a result, salience increases the recognition and evaluation of dangers, as users act and think more cautiously in their everyday encounters with the IS as they become more sensitive to subtle irregularities. Regularly confronting users with cyber security risks and drawing their attention to them is a viable strategy for increasing their visibility (e.g., through regular workshops). Risk identification and evaluation facilitates the internalization of responsibility. This was also demonstrated by our findings, as respondents who were aware of possible threats typically reported feeling responsible for the cyber security of their firms.

IT capabilities: Critical to cyber security are the users' IT capabilities (i.e., their ability to respond properly to threats or incidents) [2]-[33]. Our findings demonstrated that capabilities are bolstered by user awareness, since knowledge of cyber security risks and potential countermeasures lays the groundwork for avoiding such risks and implementing suitable countermeasures in the event of cyber security incidents. In addition to awareness, inexperience and knowledge play a significant impact in IT capabilities. The acts of inexperienced users cannot be based on comparable instances from the past. Therefore, lack of experience is negatively associated with expertise. In this instance, knowledge indicates the users' capacity to respond correctly to an issue. Only through exposure to similar real-

world situations or via hands-on training can expertise be acquired. Users with limited knowledge and experience run the risk of misjudging their own actions, which limits the growth of their powers. Our investigation revealed that inexperienced users have a tendency to evaluate their own acts as (too) positively and, as a result, sense no need to enhance their IT skills. Yet, IT skills are vital, as they have a favorable effect on the internalization of responsibility. They decrease dangerous conduct and allow for a more accurate evaluation of one's behaviors. Thus, they enhance the willingness to accept responsibility for one's acts.

Internalization of responsibility: We interpret the internalization of responsibility as the extent to which users feel accountable for their behavior and the outcomes ensuing from their usage of corporate IT [12]-[15][29]. This indicates that users not only notice hazards, evaluate them, and respond to them, but also feel accountable for exhibiting a particular behavior. This component has the following subdimensions: Externally imposed responsibility is the level of perceived obligation that is externally assigned and communicated to users within their organizational job. In addition, there is the expected division of responsibility between the organization (i.e., the IT department/IT managers) and the users (i.e., the degree of responsibility users assume to apply to them). The more accountability that is externally imposed on users (e.g., through measures that prohibit or reward undesirable conduct), the more responsibility they assume for themselves. Lastly, there is accountability felt internally, or the degree to which users feel responsible for their activities. Internally perceived responsibility is connected to responsibility allocation. The more responsibility consumers believe they must assume relative to the organization, the more they will internalize that duty. We contend that internalization of responsibility is positively associated with desirable user conduct.

User behavior: Organizational cyber security behavior encompasses acts and avoidance in regard to cyber security measures. User behavior is essential to organizational cyber security due to the socio-technical nature of cyber security [8]-[12]. Three relevant subdimensions for desirable user behavior in the current setting were extracted from the data. First, there is the adoption and observance of security measures, i.e., the IT department's technological security measures, such as regular password changes and spam filters. Second, compliant user IT behavior, such as acts that adhere to the organization's policies and cyber security guidelines, is crucial. This involves the usage of antivirus software and appropriate behavior when dealing with phishing communications, for example. Lastly, there is the active participation of users to IT security, such as the reporting of questionable instances. These three subdimensions of ideal user behavior can be viewed as three stages that arise as users acquire more knowledge and experience. Acceptance of security measures is a relatively passive kind of support for an organization's cybersecurity strategy, but IT-compliant conduct and notably active contributions to IT security are active forms of support for the organization's cyber security by its users.

Organizational IT: Cyber security-related portions of an organization's IT environment are referred to here. Particularly, we concentrate on components that can influence desirable user behavior, such as the cyber security infrastructure, the organizational responsibility for cyber security, and the corporate cyber security plan. Often, the IT department has the overall responsibility for a safe IT environment inside a business. This job includes designing and maintaining the IT infrastructure so that its software and hardware are secure. In addition, this obligation includes the creation and maintenance of a cyber security strategy that includes actions that can directly influence user awareness, IT capabilities, and the internalization of responsibility. Specifically, our interviews demonstrated that discussing commonly attacked IT infrastructure components and the types of assaults increases user knowledge and provides a foundation for enhancing IT capabilities (e.g., recognizing phishing mails). Also, the cyber security strategy can define the extent to which cyber security trainings are provided to enhance IT capabilities. In addition, it contributes directly to the internalization of responsibility by establishing the degree of responsibility distribution and by externally imposing responsibility through active communication, emphasizing consequences and rewards for non-compliant and complying behavior, respectively.

6. Discussion

6.1. Implications for research and practice

Our findings have two significant implications for organizational cyber security. Secondly, we present an integrated, comprehensive model for organizational cyber security management by integrating fragmented literature with the results of our qualitative study. Based on our qualitative data, we elaborated on the interrelationships between the model's components (see 5. Model development). With these extended interrelationships, we demonstrate how desirable user behavior plays a vital role in the socio-technical context of corporate cyber security, and how user awareness, user IT skills, and particularly internalized responsibility shape behavior in this context. Thus, we contribute new insights to the ongoing discussion on the understanding of cyber security compliance [7]-[23] and offer new potential explanations for why users behave in organizational contexts in ways that are desirable in terms of cyber security guidelines and policies.

Second, we demonstrate that internalization of responsibility is a fundamental concept for desirable user behavior in cyber security and may be viewed as a stage between user awareness and real user conduct. With the internalization of responsibility, we included an existing notion [29] into our model, which we then expanded by incorporating the perceived allocation of responsibility. We suggest that this more accurately reflects the reality of organization and user duties. Moreover, this demonstrates the advantages of shared responsibility, as described by [12]. In accordance with [25], the reported results indicate that a sense of personal responsibility has a favorable effect on behavior and contributes to security compliance. Yet, internalizing accountability demands user knowledge and IT skills. Our results reflect prior findings that in the absence of user awareness or poor user IT skills, accountability is not internalized and users do not exhibit desirable, i.e. cyber security compliant, behavior [25].

We also provide numerous implications for application. We demonstrated that increasing awareness factors, such as user knowledge or targeted awareness efforts, had a good impact [1. This enhances the recognition and appraisal of hazards, which has a favorable impact on the internalized responsibility of the users. The survey demonstrates that user education is crucial, as the majority of respondents assessed their own knowledge as inadequate and their levels of experience and expertise as low. To promote users' internalization of responsibility, user- and context-specific seminars and practical training examples are required. In addition, enterprises should explicitly convey user responsibility expectations. This raises the externally imposed accountability and gives consumers the impression that they are genuinely accountable for their behavior. This can be accomplished with periodic reminders and tailored IT guidelines containing clear expectations and recommendations.

A combination of strategies comprising knowledge transfer, training, continual support, and an incentive system that depends on rewards and deterrence will produce the maximum possible results for enterprises. To actively move user behavior in a desirable direction, however, it is necessary to specify what desirable behavior consists of and how it is measured. In this instance, desired behavior refers to compliance with CEPU's cyber security rules, such as keeping antivirus software up-to-date, routinely changing passwords, avoiding suspicious links, and reporting questionable e-mails. Possible metrics for measuring the level of desirable user behavior could include the number of events caused by human (mis-)behavior, the percentage of users with outdated antivirus software, the number of cyber security trainings, and the number of suspicious e-mails reported.

6.2. Limitations and Further Research

The interviews with CEPU members offered us a solid introduction to the topic. Nevertheless, all participants in this study belonged to the same firm, which limited the diversity of user and IT management opinions. Although the CEPU is equivalent to a business in terms of organizational complexity and processes, university IT systems are created more transparently than those in businesses. In a business setting, users may also demonstrate higher levels of felt responsibility than university students.

Future studies should examine the internalization of responsibility in greater depth. Here, we have taken the initial step. Yet, we require a more thorough development of the notion and a more explicit characterization of the scope of user accountability. In addition, it should be explored in greater depth if further components have been overlooked from this study. External elements such as the user's operating environment, demographic factors such as age, gender, and country of origin, and societal factors such as internalized values and conventions are possible. Moreover, it should be mentioned that the responsibility of users in the context of cyber security in companies requires greater theoretical and practical consideration in order to effect lasting changes in user behavior.

7. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84(2), 191–215.

[5] Barker, G., & Barker, P. (2019). Developing Cybersecurity Culture: The Role Of Cultural Values In Organizational Cybersecurity Compliance And Risk Management. Computers & Security ,Vol.82, 165-175.

[6] 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.

[7] Chen, Y., & et al. (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.

[8] 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.

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

[10] 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.

[11] 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.

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

[13] 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.

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

[15] Filipczuk, D., Mason, C., & Snow, S. (2019). Using a Game to Explore Notions of Responsibility for Cyber

Security in Organizations. CHI Conference on Human Factors in Computing Systems, , 1-6.
[16] Gallagher, R., Jones-Wilson, T., & Smith, B. (2018). Cybersecurity: Best Practices And Standards For Small Businesses. Journal Of Business & Economics Research , Vol.16(3), 109-118.
[17] 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.
[18] Glaser, B. G. (2002). Conceptualization: On Theory and Theorizing Using Grounded Theory. . International Journal of Qualitative Methods, 1(2), 23–38.
[19] Gupta, A., & Hammond, J. (2019). From Data Breaches To Disasters: Understanding The Importance Of Corporate Accountability For Cybersecurity . Journal Of Business Ethics , Vol.160(2), 399-412.
[20] Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. . European Journal of Information Systems, 18(2), 106–125.
[21] Hobson, S., & van Schaik, S. (2017). Internalized responsibility: What is it? . Journal of Applied Psychology Research, 5(1), 24–29.
[22] IBM Security, & Institute, P. (2021). Cost Of A Data Breach Report . Retrieved from www.ibm.com: https://www.ibm.com/security/data-breach
[23] Jenkins, J., & al., e. (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.
[24] Lambert, C., Lecky- Thompson, L., Marrington-Reece, J., & Carswell, J. (2018). The role of internalized responsibility in cyber security threats: A qualitative study. International Journal of Information Management, 38(6), 772–783.
[25] LaRose, B. R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. . Communications of the ACM, 51(3), 71–76.
[26] 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.
[27] National Institute Of Standards And Technology [NIST]. (2017). Framework For Improving Critical Infrastructure Cybersecurity Version 1.1.
[28] 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.
[29] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41.
[30] Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. MIS Quarterly, 34(3), 503–522.
[31] Strauss, A., & Corbin, J. (1990). Basics of grounded theory methods. Sage.
[32] 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.
[33] 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.
[34] http://www.ccs.neu.edu/home/pb/mud-history.html. 1986. (URL link *include year)
[35] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representation," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS '07), pp. 57-64, Apr. 2007, doi:10.1109/SCIS.2007.367670. (Conference proceedings)

Author Profile

Among my academic credentials, I hold a B.S. as well as a M.S. degree from 2000 to 2005 in Computer Science, as well as a PhD in Cyber Security Administration from Charisma University in 2022. I have been working in the field of Cyber Security since 2006, and I have also been granted patents under my name. It was my privilege to assist many Master's students with the selection of their thesis topics and to offer guidance on how to develop their proposals. Among the students were students from Sweden, France, and Lebanon. As a Ph.D. student, I assisted in the development of the thesis in Bulgaria, France, and the United States.