Motivational Factors in Cybersecurity: Linking Theory to Organizational Practice

Tobias Reittinger[0000−0001−7458−9928], Magdalena Glas[0000−0003−0239−7526], Sarah Aminzada[0000−0001−9537−4328], and Günther Pernul[0000−0003−1338−9003]

University of Regensburg, Regensburg, Germany
{tobias.reittinger,magdalena.glas,sarah.aminzada,guenther.pernul}@ur.de

Abstract

Purpose – This study investigates the application of motivational strategies to encourage security-compliant behavior among employees in organizational cybersecurity exploring how organizations motivate security-compliant behavior among employees in Germany. It aims to bridge the gap between theoretical motivational models and practical implementation within organizations.

Methodology – The research employs a qualitative approach, conducting semi-structured interviews with 18 participants from organization of different sizes and sectors in Germany, illuminating the topic from three perspectives: Executive managers, security specialists, and regular employees. A deductive analysis is applied to coding the interview along intrinsic motivators (competence, relatedness, and autonomy) and external motivators (incentives and nudges).

Findings – The study found that some motivational factors, such as positive incentives like vouchers, and a healthy error culture effectively lead to employees being motivated to follow security guidelines. Conversely, we found several aspects that employees perceive as frustrating and ineffective, such as compulsory e-learnings or overcomplex security policies, hindering their intrinsic motivation to contribute to organizational cybersecurity.

Originality – While existing literature offers insights into specific motivational methods applied within organizations, this paper is the first to adopt a broader perspective by analyzing how organizations' cybersecurity strategies integrate both intrinsic and extrinsic motivational approaches.

Keywords – Cybersecurity, Motivation, Incentives, Nudges, Awareness, Compliance, Policy.

Paper Type – Research paper

1 Introduction

As today's digital landscape evolves rapidly, the threat of cybercrime is ever-growing. In 2023, the reported costs of cyberattacks amounted to 8.15 billion US dollars, estimated to rise to over 13 billion US dollars by 2028 [37]. Most of these attacks target employees as entry points to infiltrate organizational systems or extract sensitive information, e.g., through phishing or stolen credentials [40]. To this end, organizations must recognize their employees' essential role in maintaining a robust cybersecurity posture, acting as the "last line of defense" against cyberattacks [24,6]. This makes it vital that employees understand and adhere to cybersecurity policies [35]. Hence,

exploring ways to motivate employees toward security-compliant behavior emerges as a critical challenge. While existing literature provides theoretical methods for improving individuals' intrinsic and extrinsic motivation in this regard [42,7,11], there is a lack of research examining how these strategies are implemented in current organizational settings (see Section 2). Thus, we raise the following research question:

RQ. *How do organizations motivate employees toward security-compliant behavior?*

To address this research question, we conducted a study in Germany, a leading economic country with a diverse landscape of organizations. Through semi-structured interviews with 18 participants drawn from organizations of varying sizes and industry sectors, we capture insights from three organizational perspectives: Executive managers, security experts, and regular employees. We use a literature-based classification scheme to categorize the identified strategies and examine their efficacy in improving the organizational security posture based on the participants' experiences. Through this analysis, we outline ways for enhancing and complementing existing strategies, aiming to provide organizations with actionable insights on effectively motivating employees toward security-compliant behavior.

The remainder of this paper is structured as follows. In Section 2, we provide the theoretical foundation of this work. Section 3 outlines our methodology for conducting and analyzing the semi-structured interviews, followed by presenting our findings in Section 4. We then discuss the conclusions drawn from these findings in Section 5 and conclude this work in Section 6.

This work represents an extension of the research we presented at the International Symposium on Human Aspects of Information Security and Assurance 2024 and which is published in the corresponding proceedings [30]. As such, we could extend the background and related work section (see Section 2), giving the reader a more comprehensive overview of existing theories and literature in the field. Additionally, this extended version allowed us to include more findings drawn from the interviews (see Section 4) and extend the recommendations for organizations (see Section 5) accordingly.

2 Background and Related Work

We outline the theoretical background and related work in the following.

2.1 Motivational Theory

To categorize motivational strategies, we employ Self-Determination Theory (SDT) as proposed by Ryan and Deci [33]. SDT offers a framework for understanding human motivation by distinguishing between *intrinsic motivation* and *extrinsic motivation*. Intrinsic motivation, which arises from an internal interest in an activity, fosters long-term commitment and is enhanced by fulfilling three basic psychological needs: *competence*, *relatedness*, and *autonomy*. Specifically, competence entails a sense of mastery in one's actions, relatedness involves forming meaningful interpersonal connections, and autonomy refers to experiencing volition in one's behavior. Although organizations cannot directly shape employees' experience of autonomy, they can modify the work environment to promote intrinsic motivation [10]. In contrast, extrinsic motivation derives from external rewards and punishments and effectively drives short-term behavior. However, its use should be approached with caution, as overreliance on external incentives may undermine

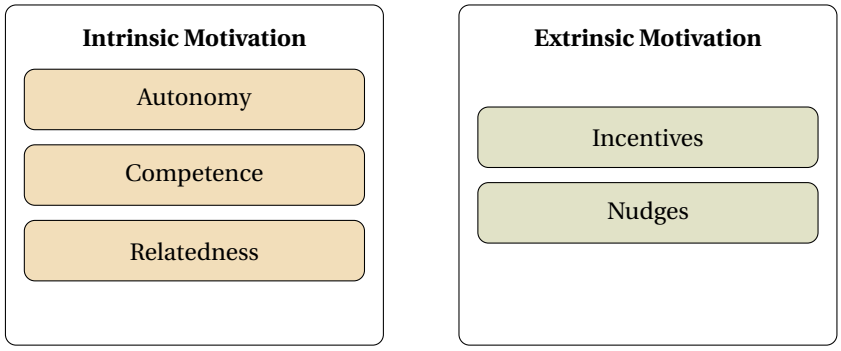

Fig. 1. Categorization of motivational strategies based on SDT [33] and Thaler and Sunstein [38].

intrinsic motivation. Extrinsic motivation can be reinforced through two primary mechanisms: *incentives* and *nudges* [33,38]. Incentives are designed to influence behavior by offering rewards or imposing penalties, whereas nudges are subtle cues that encourage desired decisions without restricting individual choice [38]. Examples include information visibility nudges, which highlight relevant details; choice-default nudges, which preset options to guide users toward specific decisions; messenger reputation nudges, which leverage the credibility of the communicator to underscore the importance of a message; and social reference nudges, which highlight how peers behave and thus lowering the perceived barrier to actions [22,20]. In the cybersecurity domain, applying SDT enables organizations to cultivate long-term commitment by fostering intrinsic motivation, thereby encouraging employees to adopt security-compliant behaviors based on a personal conviction in the value of these practices [11]. Additionally, organizations can strategically employ extrinsic motivation to promote short-term security compliance [17]. Figure 1 illustrates the categorization of these motivational strategies. In this paper, we define *motivators* as the factors that organizations can leverage to enhance employees' motivation toward security-compliant behavior.

2.2 Related Work

Several studies have advanced the understanding of employee motivation in organizational cybersecurity. Pham et al. [28], employing a methodology similar to ours, found that IT environments often demotivate employees. Two conceptual studies by Gangire et al. [11] and Fisher et al. [7] highlight the potential impact of employees' intrinsic motivation on security-compliant behavior, drawing on existing literature. Empirical research further examines the influence of intrinsic motivation on adherence to security protocols: for instance, Yang et al. [42] showed that intrinsic motivation, as described by Self-Determination Theory (SDT), encourages security compliance, though their findings were limited to employees' willingness to adopt password managers. Li et al. [25] investigated how cybersecurity awareness, corresponding to the SDT factor *competence*, shapes cybersecurity behavior, demonstrating that better-informed employees are more likely to act in a security-compliant manner. In contrast, Reeves et al. [29] focused on negative motivators, revealing that excessive security training or forced security measures (e.g., frequent password changes) can lead to "security fatigue" and, consequently, non-compliant behavior. On the other hand, Goel et al. [16] examined extrinsic motivators, finding that financial rewards and penalties

increase security compliance. Reittinger and Pernul [31] proposed a taxonomy of cybersecurity incentives, presenting a range of extrinsic motivators organizations can employ. Additionally, Renaud and Zimmermann [32] found that nudges encourage users to select stronger passwords, and Golla et al. [17] noted a similar effect in increasing the adoption of two-factor authentication. Baumer et al. [3] further demonstrated that digital nudges can significantly alter employees' behaviors during access reviews. Overall, prior research has either taken a purely theoretical approach or zeroed in on specific motivational factors (such as *competence*) or discrete areas of security compliance. By contrast, our study adopts a broader perspective, exploring how diverse organizations implement motivational strategies to encourage security-compliant behavior. We compare our findings to these earlier works to contextualize our results within the larger literature, identify common ground, and highlight opportunities for organizations to refine their motivational strategies.

3 Method

In this section, we describe our methodology. We chose semi-structured interviews [1] to engage participants in an open discussion on their experiences with employee motivation in organizational cybersecurity. We explored the topic from three different perspectives: *Managers*, who hold leadership positions within organizations, *security specialists*, who are professionals responsible for security measures, and *employees*, who comprise organizations' broader workforce.

3.1 Participant Recruitment

To ensure participants are from all three perspectives, we used purposive sampling for the recruitment. Suitable participants were recruited from the authors' professional networks. We aimed to recruit participants from various industrial sectors and organization sizes to capture a broad spectrum of experiences. Participants were not compensated for their participation. We stopped recruiting after the interview findings reached saturation, as described below. The final sample consists of 18 participants with four *managers*, five *security specialists*, and nine *employees*, all from Germany. Participants are described in Table 1.

3.2 Interview Structure

In the questionnaire development, we deliberately avoided questions about specific types of motivational approaches or SDT so as not to bias their answers. First, participants described their general demographics. Subsequently, participants shared their general perceptions of the security culture within their organizations. This enabled us to establish a foundation for the discussion and provide context for understanding participants' perspectives. Next, an open dialogue was facilitated to explore the strategies employed by their respective organizations to enhance employee motivation, as well as areas they identified for potential enhancement. The interview questionnaire is presented on GitHub.[1]

[1] https://github.com/employee-motivation/questionnaire

Table 1. Summary of our 18 interview participants' demographics.

ID	Job title	Sector	Employees	Gender	Exp.
M1	CEO	Retail	10-99	M	35
M2	CEO	Consulting	100-999	F	10
M3	Head of department	Construction	1,000-9,999	F	9
M4	Doctor	Healthcare	10-99	M	22
S5	CISO	Financial Services	100-999	M	8
S6	Security Architect	Infrastructure	1,000-9,999	M	6
S7	Head of department	Metal processing	1,000-9,999	M	6
S8	CISO	Infrastructure	+10,000	M	12
S9	Security Consultant	Software development	1-9	M	10
E10	Engineer	Metal processing	1,000-9,999	M	3
E11	Administration	Public administration	100-999	F	5
E12	Graphic Designer	Consulting	100-999	M	7
E13	Chemist	Chemical industry	1,000-9,999	M	1
E14	Researcher	Public administration	1,000-9,999	M	2
E15	Administration	Construction	1,000-9,999	M	2
E16	Accountant	Public administration	+10,000	F	9
E17	Financial Advisor	Financial Services	100-999	F	17
E18	Medical assistant	Healthcare	10-99	F	6

Note. IDs beginning with *M* refer to *management*, *S* to *security specialist*, and *E* to *employee* positions.

3.3 Interview Procedure and Ethics

The interviews were conducted by two of the authors between October 2023 and March 2024. 14 interviews were held remotely via Zoom or Microsoft Teams, and four were conducted in person. For interviews where participants agreed, we conducted audio recordings, which were later transcribed for the analysis. If this was not feasible (M4, S9, E16), we manually captured participants' responses during the interviews. The interviews lasted, on average, 40 minutes.

Before conducting our study, the study design was approved by the *German Association for Experimental Economic Research*, and we obtained an Institutional Review Board (IRB) certificate.[2] Participants consented to participating and to recording the interviews. After the transcription, we deleted the audio recordings and anonymized participants' affiliations to preserve their privacy.

3.4 Coding and Analysis

To analyze the use of strategies to motivate employee motivation in cybersecurity, we used a deductive analysis approach [4] to map interview data with the theory-based classification of employee motivation introduced in Section 2. This classification served as an initial codebook.

[2] The IRB certificate is available online: https://gfew.de/ethik/MwJFdwPK

Two authors refined the coding structure through multiple rounds, resolving conflicts with flexible coding [5]. After 18 interviews, no additional code was created, indicating that the analysis reached saturation and further interviews would likely yield no further insights.

3.5 Limitations

We acknowledge our methodology's limitations. The geographic scope of the interviewees was limited to Germany. While this might restrict the generalizability of the results to other countries, it allowed for a focused exploration of employee motivation for security practices within the German context. Future research could validate our results in different regions. There is also the possibility of self-reporting bias, particularly among managers and specialists, which may affect the data's accuracy. To mitigate this limitation, we interviewed participants from diverse organizations and only stopped as the coding reached saturation.

4 Findings

In this section, we present the identified motivators of the interviews. As introduced in Section 2, we distinguish between two types of motivators. First, *intrinsic motivators* are internal factors that engage employees in long-term security-compliant behavior based on personal interest and the activities' inherent satisfaction. In contrast, *extrinsic motivators* are external factors that drive short-term security-compliant behavior based on rewards or encouragement.

4.1 Intrinsic Motivators

In the following, we describe intrinsic motivators we identified in the interviews, classified by the three categories *competence*, *relatedness*, and *autonomy*.

Competence. Organizations can encourage employees to adhere to security-compliant behaviors by implementing cybersecurity education programs. All the interviewees' organizations offer some sort of cybersecurity awareness training for their employees. Organizations typically test the knowledge gained from a training course in an assessment. Half of the organizations offer training solely when hiring employees. One employee summarizes the experience:

Organizations can encourage employees to adhere to security-compliant behaviors by implementing cybersecurity education programs. All interviewed organizations offer some form of awareness training, and most of them assess employees' newly acquired knowledge after the training. Half of the organizations provide this instruction only when employees are first hired, potentially limiting its effectiveness over time. In addition, making employees aware of real-world security incidents, particularly those at suppliers or within the broader industry, can further enhance motivation by illustrating that this can happen to every organization. Such tangible examples help employees grasp the seriousness of potential threats and reinforce the need for security-compliant behavior. One employee summarizes the training experience:

> *"I only had one training course at the beginning of my employment. Little of it has stuck [...] and a refresher wouldn't hurt."* (E17)

In contrast, the other half of the organizations conduct cybersecurity training on an annual basis. While research underscores the importance of periodic sessions for preserving employees' cybersecurity competence [19], many participants reported difficulties applying the training to their everyday tasks. They struggle to derive benefits for their daily work and often perceive it as an additional burden. Moreover, several participants emphasized that perceived relevance plays a crucial role in motivating engagement. As one employee explained:

> *"There is often discussion about the usefulness of the training courses, as the relevance is not recognized. This can increasingly be observed among colleagues who are not IT-savvy."* (E10)

Additionally, participants noted that much of this training remains overly generic, covering basic cybersecurity best practices with limited relevance to their day-to-day responsibilities. As a result, one participant explained the following:

> *"[...] most people just endure the training and then go back to doing whatever for the rest of the year."* (E11)

Some training courses offer gamification and serious games. Through a playful environment, organizations want to engage their employees to gain knowledge in a hands-on environment. Yet, not all employees are fond of gamification and serious games. Interviewees reported that younger employees enjoy playing serious games but noted older employees prefer a more neutral learning environment with fewer distractions. One participant explains the perception of a serious game:

> *"[...] quiz questions and mini-games that older employees comment on with little enthusiasm"* (E10)

Managers and security specialists have also recognized the different training requirements of different employee groups. Still, the same training content is typically used for all employees. This has disadvantages for the training's effectiveness, as a manager acknowledges that many employees cannot derive benefits from it for their daily work.

Interviewees' of large organizations reported they are regularly exposed to phishing simulations. These simulations have two objectives. First, they want to check employees' knowledge levels to adjust the scope of training accordingly. Second, employees' awareness is raised as they know that they regularly receive phishing emails and develop a routine of reporting emails. Employees recognize the positive effect of increased awareness and are not bothered by phishing simulations, as they take up little time in their day-to-day business.

Furthermore, all the interviewees' organizations have security policies that aim to guide employees toward security-compliant behavior, such as rules for passwords or the use of USB sticks. However, acceptance of these policies is perceived differently across roles: while security specialists view acceptance as high, employees feel it is generally low. As a result, employees report facing practical challenges with those guidelines:

> *"The security policies are a 10-page document with countless regulations. As a result, I am unsure what I can and cannot do."* (E11)

Although employees know that there are security policies, some interviewees reported that they are unaware of where they are stored and how to access them. To summarize, organizations lack personalized training to continuously educate employees and comprehensible security policies.

Relatedness. The interviewees agree that the more employees feel connected to the organization, the more likely they are to protect the organization and, thus, behave in a security-compliant manner:

> *"A happy employee is more attentive and likely to report [...] if something seems strange or if they have clicked on a suspicious link."* (M1)

Additionally, organizations encourage relatedness by strengthening cooperation and a sense of belonging among employees, emphasizing that cybersecurity is a collective responsibility. As one participant explained:

> *"Everyone understands that security risks are also business risks and that we can only manage them together."* (S8)

In detail, organizations pass on reported incidents via their intranet, as attackers typically try different places in the same organization. This practice spreads crucial information and initiates open discussions on cybersecurity matters within the workplace. In addition, some employees reported an open information culture among the organizations' workforce, where they openly discuss uncertainties about cybersecurity practices and incidents that have occurred in the organization with their colleagues.

Despite ongoing efforts to promote teamwork and collective responsibility, many employees noted a lack of relatedness in their organizations' cybersecurity initiatives. They stressed that visible commitment from managers is essential for motivating the workforce to take cybersecurity seriously. When senior leadership does not treat cybersecurity as a core business concern, employees' sense of organizational belonging fails to translate into secure behaviors. One interviewee remarked:

> *"Managers dismiss awareness training as a gimmick and demand that employees clock out."* (E10)

According to participants, such an attitude diminishes the perceived importance and value of security training, ultimately undermining employees' motivation to remain vigilant. They called for a reversal of this pattern, emphasizing that executives should model responsible cybersecurity practices. As another participant explained:

> *"C-Levels are not even aware that they have to take cybersecurity into their own hands. They see it as a task of the security department."* (E12)

By actively exemplifying cybersecurity as a shared responsibility, managers can reinforce the importance of secure practices and foster a stronger sense of relatedness across the organization. In sum, relatedness can foster security-compliant behavior, but often, management lacks cybersecurity commitment, diminishing employees' relatedness.

Autonomy. Many employees reported feeling that their autonomy in security-related practices is overly restricted. Training sessions, for instance, are often compulsory and include mandatory assessments. This obligatory format can sap employees' motivation, as it shifts their focus from genuinely learning to merely completing the course:

> *"The mandatory training is an additional burden in day-to-day business. One colleague even had the training done by an intern."* (E10)

While interview participants recognize the importance of mandatory security training, many still find it frustrating:

> *"People get it, but it still gets on their nerves."* (E13)

This frustration also extends to certain security policies—such as mandatory password changes every three months—that aim to enhance security but often yield superficial compliance. By compelling frequent password updates, some organizations inadvertently encourage minimal adjustments rather than meaningful improvements:

> *"I comply with the mandatory password change by adding a single character or adjusting the capitalization. I think it's doubtful whether the rule makes sense at all, [...] but I have no choice."* (E12)

In short, a culture of enforced cybersecurity measures could lead to a superficial compliance. Instead of genuinely bolstering security, these rigid rules can undermine it by fostering resentment and habitual workarounds. Notably, several security specialists reported better outcomes when granting employees more flexibility, such as selecting their own password management strategies within certain guardrails. This added autonomy helps employees perceive these requirements not as arbitrary burdens, but as meaningful steps to protect their organization. Striking a balance between firm guidelines and reasonable freedom can alleviate frustration and cultivate a more proactive, security-conscious culture.

4.2 Extrinsic Motivators

As outlined above, extrinsic motivators can effectively promote a timely shift in employee behavior. In the following, we describe the identified extrinsic motivators classified by the two categories *incentives* and *nudges*.

Incentives. Most organizations within our study avoid negative incentives, like punishments, for employees who have made a mistake in cybersecurity. Organizations recognize the value of a positive error culture, where mistakes are viewed as an opportunity for improvement. This approach encourages employees to report security incidents without fear of sanctions, as one manager articulated:

> *"Who clicks is a victim, not a perpetrator. [...] We live a healthy error culture. No employee is punished for making unintentional mistakes. Employee reportings help us immensely, so we want to facilitate it."* (S8)

Yet, implementing a healthy error culture is not successful in all organizations. In some cases, employees must pass additional mandatory training if they make a mistake, which is perceived as a punishment. Employees stated that sanctions diminish their motivation to act security-compliantly and report security incidents. One employee even reported being scared of the security department.

Regarding positive incentives, some interviewees' organizations have introduced bonus programs to motivate proactive cybersecurity behaviors. These initiatives reward employees for reporting phishing emails or suggesting improvements to cybersecurity practices. The prospect of receiving a voucher for the most submitted reports encourages employee awareness and reporting commitment. An interviewee shared their experience:

> *"Before [the bonus program], we simply deleted potential phishing emails. Now we report them with the phishing button in Outlook and can win a voucher as a result."* (E17)

While incentives can increase reporting and positively shift employee behavior, they also have downsides, including higher processing efforts and costs for IT departments. Yet, managers view these as acceptable trade-offs for enhancing cybersecurity and maintaining an incident-free reputation. A management participant elaborates on this balance:

> *"The numerous reports cause a higher efforts in our IT department, which results in higher costs. But it's worth the positive reputation."* (M2)

Furthermore, employees describe that their motivation to report suspicious activities or emails greatly increases when they know that the organizations use their reports and have value. Interviewees are also uncertain whether their reports are actual incidents or false positives. Thus, feedback would be an incentive for employees and could improve their competence. Yet, employees often lack a response, which can lead to disillusionment, as one noted:

> *"I often report emails via the phishing button, but nothing happens, which is demotivating. It feels as if [...] my efforts are for nothing."* (E18)

Timely feedback for reported security incidents not only acknowledges employees' efforts but can also reinforce the learning process:

> *"Although my reports are processed by IT, it takes several weeks to receive feedback. I can no longer remember what I reported. [...] The learning effect would be greater if I received feedback more quickly."* (E17)

In summary, establishing a healthy error culture, creating rewards for proactive cybersecurity behavior, and leveraging employee commitment were identified as compelling incentives for cybersecurity within the organization.

Nudges. Information visibility nudges are widely used in organizations to heighten employee awareness of potential security threats. For instance, many email programs display prominent warnings, such as a red banner, to indicate when messages originate from outside the organization. As one security specialist explained:

> *"Employees are often careless and click on links and open attachments from external untrusted senders. We want to increase awareness with a red banner so employees read the message more carefully."* (S5)

By prompting employees to scrutinize external emails more thoroughly, these nudges can help reduce careless interactions with potential phishing attempts. However, the lack of granularity in how these warnings are applied diminishes their overall effectiveness. According to multiple interviewees, all messages from external senders receive the same alert—regardless of their actual risk level. Our interviewees described that this implementation has inadvertently led to security fatigue, as they feel overwhelmed by constant alerts and start to disregard these warnings. An employee described their experience:

> *"Every email from a customer has the same warning. Initially, I read every message cautiously, now I hardly see the warning anymore."* (E12)

Beyond highlighting potential risks, some organizations have introduced a social reference nudge to encourage reporting of security incidents and suspicious emails. One security specialist (S5) described using a social reference nudge, showing how many colleagues have submitted reports. This approach leverages the human tendency to *follow the herd* [22], signaling that reporting suspicious emails is common among the colleagues. As the specialist noted, reporting rates increased once employees realized many of their peers were also taking action.

Overall, nudges can promote security-compliant behavior of employees, as they guide them toward more secure decisions. Nonetheless, overuse of nudges may cause security fatigue and reduce their effectiveness.

5 Discussion

We now discuss our findings and offer recommendations for organizations to motivate employees toward security-compliant behavior in the long term. We map our recommendations with the different types of motivators in Table 2.

5.1 Management Commitment

Organizations need to adapt their security culture to motivate employees to comply with security policies, as outlined by Mwin and Mtsweni [26]. They emphasize that cybersecurity is a collective responsibility, with every employee potentially representing a security vulnerability. The fighter analogy by Solms et al. [35] offers an effective way to communicate this concept to employees. Inspired by firefighting principles, this approach involves training employees to detect and address security incidents, similar to how firefighters extinguish fires to protect their organization. Within this analogy, every employee becomes a security fighter capable of

Table 2. Mapping of our recommendations with the different types of motivators.

Recommendations	Intrinsic Motivators			Extrinsic Motivators	
	Competence	Relatedness	Autonomy	Incentives	Nudges
Management Commitment		•			•
Personalized Education	•		•		
Comprehensible Policy	•		•		•
Using Employee Reports	•	•	•	•	•

identifying and mitigating cybersecurity threats. This analogy can help build a culture where all employees recognize themselves as contributors to organizational security, fostering ownership and empowerment.

Organizations can further support this cultural shift by employing *messenger reputation* nudges to promote the analogy of cybersecurity as a shared responsibility. Jesse and Jannach [22] emphasize that employees are more inclined to follow the lead of people they respect and trust. By doing so, leaders motivate employees to adopt secure behavior and reinforce their central role in safeguarding the organization. Improving this sense of relatedness can integrate cybersecurity into everyone's job responsibilities.

However, our study, in line with prior research [21], shows that these approaches often lack support at the management level. When executive leaders are not involved and lack an understanding of cybersecurity, it is frequently perceived as a mere cost rather than a vital part of the organization's IT strategy. This perception may stem from insufficient cybersecurity expertise among executives [18,27,36]. Therefore, a comprehensive cybersecurity strategy should not only engage executives in decision-making but also enhance their competence through tailored initiatives and awareness programs. Programs such as cyber range exercises offer practical opportunities for executives to experience simulated cybersecurity incidents, enabling them to understand the impact of real-time threats and the importance of proactive security measures [13,15]. Through such initiatives, executives can make better-informed decisions, ensuring that cybersecurity is recognized and prioritized as a critical component of the organization's long-term success.

5.2 Personalized and Voluntary Education

Li et al. [25] identified that better-educated employees adhere more to security policies and are more aware. However, in the evolving cybersecurity landscape, training methods often fall short, presenting learning material that is too complex and abstract for the diverse needs of employees [2]. These one-size-fits-all programs often disregard the fact that employees come with varying degrees of technical expertise, perform different roles, and operate under diverse workloads, leading to suboptimal learning outcomes. An effective approach could be to tailor the content and difficulty of training materials to employees' current knowledge levels and specific responsibilities, ensuring that instruction remains relevant, accessible, and appropriately challenging. In particular, it could be vital to illustrate how small errors can escalate into major security breaches, underscoring the real-world consequences. Sharing examples of actual attacks

within the same industry or among suppliers, along with their underlying causes, could further explain the impact that seemingly minor oversights can have.

Additionally, serious games have been shown to significantly enhance cybersecurity knowledge by immersing learners in interactive, problem-solving scenarios [9,8]. Although younger employees may respond more enthusiastically to these techniques, the immersive format can boost knowledge retention across all age groups. By highlighting tangible risks and everyday relevance, such targeted and engaging training strategies can motivate employees to adopt security-compliant behaviors and ultimately fortify the organization's overall security posture.

However, not all employees encounter the same cybersecurity challenges. Certain *high-risk* groups, such as those with access to highly sensitive data, critical infrastructure, or direct influence over organizational security, require specialized awareness strategies beyond standard training. Developers, for instance, regularly handle proprietary source code and other confidential information, making them prime targets for cyberattacks. Conventional training modules often fail to cover application-level vulnerabilities, secure coding practices, or the specific social engineering tactics targeting developers [12,34]. Tailored training for these groups could enhance knowledge retention and strengthen their commitment to security-compliant behavior.

Another promising alternative is using cyber range-based security awareness campaigns that offer a hands-on, immersive experience by simulating attacks, such as brute-force password cracking, to demonstrate both the threat and its organizational impact [14]. This approach helps employees understand the critical importance of cybersecurity practices, improving their ability to identify, prevent, and respond to security incidents. Beyond traditional awareness training, microlearning approaches present another promising approach by providing security guidelines at the moment of need, making security education more practical and context-driven [23].

Fisher [7] advocates for voluntary education programs rather than mandatory training. However, none of the interviewees' organizations currently offer such opportunities. While regulatory requirements may pose challenges, organizations could supplement mandatory programs with voluntary cybersecurity education. Employees eager to deepen their knowledge or specialize in specific cybersecurity areas often lack the opportunity to do so. By providing optional training courses, organizations can bridge this gap, allowing employees to pursue further education out of genuine interest rather than mere compliance. This autonomy fosters intrinsic motivation, which has been shown to substantially enhance both the effectiveness and depth of learning [39].

Generative AI (GenAI) gives organizations the potential to deliver highly personalized and voluntary cybersecurity training. While many organizations already tailor content to specific departments, such one-size-fits-all grouping may still overlook individual learning needs. By dynamically adapting the depth and complexity of materials based on each learner's progress and interests, GenAI can create more relevant and engaging experiences. However, fully individualizing GenAI-driven training requires considerable effort to account for each employee's background knowledge. As a practical compromise, organizations can develop targeted modules for distinct employee groups, such as trainees, junior developers, or senior developers, while still leveraging GenAI's adaptive capabilities to refine content within those modules. This balanced approach ensures that employees receive training suited to their roles and competencies, aiming to foster stronger motivation and more effective security-compliant behavior.

5.3 Comprehensible Security Policies

Employees in our study have asked for the security policies to be more accessible and understandable. This highlights the need for a centralized repository where the policies are widely known. By

streamlining access to security policies, organizations can ensure that every employee, regardless of their technical background, can access crucial information about their role in organizational cybersecurity.

Furthermore, the clarity and comprehension of these guidelines are vital. Often, employees are eager to comply with security measures but find themselves unable to due to the complexity or vagueness of the instructions. A simplified overview of the guidelines could substantially increase competence and, in turn, employees' motivation to comply with the guidelines. Moreover, it is essential to modernize the content of these guidelines to reflect current best practices in cybersecurity. For instance, Reeves et al. [29] suggest moving away from outdated protocols like mandatory periodic password changes to more effective and user-friendly measures. Additionally, Fisher et al. [7] argued that simplified security policies can prevent security fatigue.

Additionally, organizations can simplify employees' security policy implementation by adopting strategies that guide employees toward secure behaviors. An example is the choice default nudge. By suggesting strong passwords or enabling two-factor authentication by default, employees could be nudged into security compliance, as identified by Renaud and Zimmermann [32] and Golla et al. [17]. Such measures of combining the security guidelines with practical, user-friendly solutions can increase the willingness of employees to behave in a security-compliant manner. Simply put, making the secure choice the easiest choice can enhance an organization's security posture.

5.4 Using Employee Reports Effectively

Prior research has encouraged organizations to shift their perspective from viewing employees as a security liability to recognizing them as a key part of the solution [43]. One practical way to achieve this is by actively incorporating employee-generated security reports into cybersecurity strategies. When organizations acknowledge and act on these reports, employees gain a heightened sense of contribution and relatedness, as they see the tangible impact of their efforts. This recognition also fosters autonomy, empowering employees to continue reporting incidents and to maintain security-conscious behaviors. Moreover, offering timely and constructive feedback on submitted reports further develops employees' competence. As they learn to identify and understand emerging threats, employees become more adept at producing high-quality reports. In turn, both the organization and its workforce benefit from a stronger overall security posture, as improved reporting leads to more effective prevention, mitigation, and response to potential incidents.

Adopting a healthy error culture within the organization is crucial to motivating employees toward security-compliant behavior. While Goel et al. [16] suggest that financial punishments can increase security compliance in the short term, our interviewees report that negative incentives lead to lower security efforts among employees in the long term. When organizations do not punish their employees for mistakes, employees are much more willing to report threats and behave in a security-compliant manner. In addition, carefully considered positive incentives can complement employees' motivation. In detail, small but relevant bonus programs are unlikely to diminish intrinsic motivation and can lead to a sustained increase in the quality and quantity of reports. Thus, incentives can provide organizations with valuable insights into potential security threats.

Nudges are a valuable tool to promote security-compliant behavior. Nevertheless, the success hinges on their careful application. Overuse or poorly designed nudges can lead to security

fatigue, reducing effectiveness and potentially undermining the desired security behavior. Organizations should adopt a more nuanced approach to mitigate security fatigue and maintain the effectiveness of nudges. For instance, refining email warnings to provide more specific and relevant alerts can greatly reduce the risk of security fatigue. Instead of identical warnings for all external communications, a more differentiated approach can be more effective, such as flagging emails that are likely phishing attempts or exhibit suspicious characteristics. This strategy prevents the overload of warnings and enhances employees' overall security awareness and vigilance. Thus, nudges with a nuanced approach are promising to foster employees' security compliance.

6 Conclusion

This study aimed to analyze the application of different theoretical approaches to employee motivation in organizational cybersecurity. We identified that the organizations in scope focus on raising employees' motivation mainly through educating employees about security-compliant behavior and short-time incentives. Meanwhile, there is substantial untapped potential in utilizing motivational strategies to enhance employees' sense of autonomy and relatedness toward security-compliant behavior, as well as effectively utilizing security-related incentives and nudges. Moving forward, our future research will focus on verifying our suggested improvements. To this end, we intend to conduct studies in organizations to assess to what extent the integration of the suggested strategies can improve employee motivation toward security-compliant behavior.

Use of Generative AI

We refined the language and readability of this paper with DeepL, Grammarly, and ChatGPT (Version 4), for which we take full responsibility.[3]

Acknowledgement

This paper is part of the CONTAIN project, funded by the Federal Ministry of Education and Research as part of the German government's "Research for Civil Security" framework program (13N16586).

References

1. Adams, W.C.: Conducting semi-structured interviews. Handbook of Practical Program Evaluation p. 492–505 (Aug 2015)
2. Alotaibi, S., Furnell, S., He, Y.: Towards a framework for the personalization of cybersecurity awareness. In: Proceedings of the 2023 conference on Human Aspects of Information Security and Assurance (HAISA). pp. 143–153. Springer Nature Switzerland, Cham (2023)
3. Baumer, T., Reittinger, T., Kern, S., Pernul, G.: Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. In: Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). pp. 239–258. USENIX Association, Philadelphia, PA (Aug 2024), https://www.usenix.org/conference/soups2024/presentation/baumer

[3] We outline AI Usage Cards [41]: https://ai.uversy.com/employee-motivation

4. Bingham, A.J., Witkowsky, P.: Deductive and inductive approaches to qualitative data analysis. Analyzing and interpreting qualitative data: After the interview **1**, 133–146 (2021)
5. Deterding, N.M., Waters, M.C.: Flexible coding of in-depth interviews: A twenty-first-century approach. Sociological methods & research **50**(2), 708–739 (2021)
6. Eze, T., Hawker, N.: Cap: Patching the human vulnerability. In: Clarke, N., Furnell, S. (eds.) Proceedings of the 2022 conference on Human Aspects of Information Security and Assurance (HAISA). pp. 106–119. Springer International Publishing, Cham (2022)
7. Fisher, R., Porod, C., Peterson, S.: Motivating employees and organizations to adopt a cybersecurity-focused culture. Journal of Organizational Psychology **21**(1), 114–131 (2021)
8. Friedl, S., Reittinger, T., Pernul, G.: Digital detectives: A serious point-and-click game for digital forensics. In: IFIP World Conference on Information Security Education. pp. 129–145. Springer (2024)
9. Friedl, S., Reittinger, T., Pernul, G.: From play to profession: A serious game to raise awareness on digital forensics. In: IFIP Annual Conference on Data and Applications Security and Privacy. pp. 269–289. Springer (2024)
10. Gagné, M., Deci, E.L.: Self-determination theory and work motivation. Journal of Organizational behavior **26**(4), 331–362 (2005)
11. Gangire, Y., Da Veiga, A., Herselman, M.: A conceptual model of information security compliant behaviour based on the self-determination theory. In: Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS). pp. 1–6. IEEE (2019)
12. Gasiba, T., Lechner, U., Pinto-Albuquerque, M., Zouitni, A.: Design of secure coding challenges for cybersecurity education in the industry. In: International Conference on the Quality of Information and Communications Technology. pp. 223–237. Springer (2020)
13. Glas, M., Hilmer, C., Pernul, G.: Cyber ranges: Five use cases for improving cybersecurity skills development in organizations. IEEE Security & Privacy (2025), preprint
14. Glas, M., Messmann, G., Pernul, G.: Complex yet attainable? an interdisciplinary approach to designing better cyber range exercises. Computers & Security **144**, 103965 (2024). https://doi.org/https://doi.org/10.1016/j.cose.2024.103965, https://www.sciencedirect.com/science/article/pii/S0167404824002700
15. Glas, M., Vielberth, M., Pernul, G.: Train as you fight: Evaluating authentic cybersecurity training in cyber ranges. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (2023)
16. Goel, S., Williams, K.J., Huang, J., Warkentin, M.: Can financial incentives help with the struggle for security policy compliance? Information & Management **58**(4), 103447 (2021)
17. Golla, M., Ho, G., Lohmus, M., Pulluri, M., Redmiles, E.M.: Driving 2FA adoption at scale: Optimizing Two-Factor authentication notification design patterns. In: Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). pp. 109–126. USENIX Association (Aug 2021)
18. Haislip, J., Lim, J.H., Pinsker, R.: The impact of executives' IT expertise on reported data security breaches. Information Systems Research **32**(2), 318–334 (jun 2021). https://doi.org/10.1287/isre.2020.0986
19. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., Koshutanski, H.: Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences **10**(16) (2020)
20. Hummel, D., Maedche, A.: How effective is nudging? a quantitative review on the effect sizes and limits of empirical nudging studies. Journal of Behavioral and Experimental Economics **80**, 47–58 (2019)
21. ISACA: State of cybersecurity 2023: Global update on workforce efforts, resources and cyberoperations. Tech. rep. (2023)
22. Jesse, M., Jannach, D.: Digital nudging with recommender systems: Survey and future directions. Computers in Human Behavior Reports **3**, 100052 (2021)
23. Kävrestad, J., Nohlberg, M.: Contextbased microtraining: A framework for information security training. In: Clarke, N., Furnell, S. (eds.) Human Aspects of Information Security and Assurance. pp. 71–81. Springer International Publishing, Cham (2020)

24. Kirsch, L., Boss, S.: The last line of defense: motivating employees to follow corporate security guidelines. In: Proceedings of the 2007 ICIS conference. p. 103 (2007)
25. Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X.: Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management **45**, 13–24 (2019)
26. Mwim, E.N., Mtsweni, J.: Systematic review of factors that influence the cybersecurity culture. In: Proceedings of the 2022 conference on Human Aspects of Information Security and Assurance (HAISA). pp. 147–172. Springer International Publishing, Cham (2022)
27. Olt, C., Gerlach, J., Sonnenschein, R., Buxmann, P.: On the benefits of senior executives' information security awareness. In: Proceedings of the 2019 International Conference on Information Systems (ICIS) (2019), 25
28. Pham, H.C., Pham, D.D., Brennan, L., Richardson, J., et al.: Information security and people: A conundrum for compliance. Australasian Journal of Information Systems **21** (2017)
29. Reeves, A., Delfabbro, P., Calic, D.: Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. SAGE open **11**(1) (2021)
30. Reittinger, T., Glas, M., Aminzada, S., Pernul, G.: Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality, pp. 3–16. Springer Nature Switzerland (2024). https://doi.org/10.1007/978-3-031-72559-3$_1$
31. Reittinger, T., Pernul, G.: A taxonomy of positive incentives to motivate cybersecurity behaviors. In: Proceedings of the 58th Hawaii International Conference on System Sciences (HICSS-58) (2025)
32. Renaud, K., Zimmermann, V.: Nudging folks towards stronger password choices: providing certainty is the key. Behavioural Public Policy **3**(2), 228–258 (2019)
33. Ryan, R.M., Deci, E.L.: Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American psychologist **55**(1), 68 (2000)
34. Siadati, H., Jafarikhah, S., Sahin, E., Hernandez, T., Tripp, E., Khryashchev, D., Kharraz, A.: Devphish: Exploring social engineering in software supply chain attacks on developers. In: 2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). pp. 517–523. IEEE (2024)
35. von Solms, S.H., du Toit, J., Kritzinger, E.: Another look at cybersecurity awareness programs. In: Proceedings of the 2023 conference on Human Aspects of Information Security and Assurance (HAISA). pp. 13–23. Springer Nature Switzerland, Cham (2023)
36. Sonnenschein, Rabea; Loske, A., Buxmann, P.: The role of top managers' IT security awareness in organizational it security management. In: Proceedings of the 2017 International Conference on Information Systems (ICIS) (2017), 13
37. Statista: Estimated cost of cybercrime worldwide 2017-2028 (11 2023), https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide, accessed: 01/08/24
38. Thaler, R.H., Sunstein, C.R.: Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press (2008)
39. Vansteenkiste, M., Simons, J., Lens, W., Sheldon, K.M., Deci, E.L.: Motivating learning, performance, and persistence: the synergistic effects of intrinsic goal contents and autonomy-supportive contexts. Journal of personality and social psychology **87**(2), 246 (2004)
40. Verizon: 2023 data breach investigations report. Tech. rep. (2023)
41. Wahle, J.P., Ruas, T., Mohammad, S.M., Meuschke, N., Gipp, B.: Ai usage cards: Responsibly reporting ai-generated content. In: 2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL). pp. 282–284. IEEE (2023)
42. Yang, N., Singh, T., Johnston, A.: A replication study of user motivation in protecting information security using protection motivation theory and self determination theory. AIS Transactions on Replication Research **6**(1), 10 (2020)
43. Zimmermann, V., Renaud, K.: Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies **131**, 169–187 (2019)