Employee Motivation in Organizational Cybersecurity: Matching Theory and Reality

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. Cyberattacks pose a persistent threat to organizations worldwide. These attacks often target employees as entry points to organizational systems through tactics like phishing and credential theft. Recognizing employees as an organization's "last line of defense", motivating employees toward security-compliant behavior becomes paramount. While existing literature investigates theoretical frameworks for enhancing individuals' motivation, studies regarding their practical implementation within organizational contexts remain scarce. This paper seeks to address this research gap by exploring how organizations motivate and incentivize security-compliant behavior among employees in Germany. We conducted semi-structured interviews with 18 participants from diverse organizational backgrounds, illuminating the topic from three perspectives: Executive managers, security specialists, and regular employees. Utilizing a classification derived from existing literature, we examine our findings to identify which motivational strategies are currently implemented effectively within organizational contexts. On this basis, we offer a set of actionable recommendations on how organizations can enhance and complement existing motivational strategies.

Keywords: Cybersecurity · Motivation · Incentives · Nudges · Awareness · Compliance · Policy.

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 [23]. Most of these attacks target employees as entry points to infiltrate organizational systems or extract sensitive information, e.g., through phishing or stolen credentials [25]. 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 [14,5]. This makes it vital that employees understand and adhere to cybersecurity policies [22]. 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 [27,6,8], 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.

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 the Self-Determination Theory (SDT) proposed by Ryan and Deci [21]. SDT serves as a framework for understanding human motivation and distinguishes between *intrinsic motivation* and *extrinsic motivation*. Intrinsic motivation originates from internal interest in the activity, enables long-term commitment, and can be enhanced by *competence*, *relatedness*, and *autonomy*. According to SDT, competence involves feeling skilled in one's actions, relatedness refers to meaningful connections with others, and autonomy is experiencing a sense of volition in one's behavior. Nevertheless, organizations can't directly influence employees' experience of autonomy but adapt the work environment to encourage intrinsic motivation [7]. In contrast, extrinsic motivation arises from external rewards and punishments, effectively enabling short-term behavior. Nevertheless, the authors argue that extrinsic motivation should be used with consideration, as it can undermine intrinsic motivation if individuals become overly reliant on external factors. SDT explains that extrinsic motivation can be increased by *incentives* and *nudges*. The authors outline that incentives are designed to influence behavior and consist of positive incentives such as rewards and negative incentives like penalties. Furthermore, nudges are

subtle cues encouraging desired decisions without restricting choice [15]. For instance, information visibility nudges emphasize pertinent information, the choice default nudge sets a pre-selected option to guide users toward a particular decision, and messenger reputation nudges leverage the credibility of the messenger to enhance the message's importance [13,12]. By applying SDT in cybersecurity, organizations can foster long-term commitment through intrinsic motivation, aiming for employees to adopt security-compliant behaviors driven by a personal conviction in the significance and value of these security practices [8]. Complementary, organizations can utilize extrinsic motivation thoughtfully to drive security-compliant behavior in the short term [10]. In this paper, we identify motivators, which are motivating factors that organizations can use to increase employees' motivation toward security-compliant behavior.

2.2 Related Work

Several prior works have contributed to understanding employee motivation in organizational cybersecurity. Pham et al. [18] identified that IT environments are typically demotivating for employees, with a similar methodology to this paper. Two conceptual studies by Gangire et al. [8] and Fisher et al. [6] highlight the general potential of employees' intrinsic motivation in fostering security-compliant behavior based on the existing literature. Furthermore, several empirical studies have examined how employees' intrinsic motivation affects their adherence to security protocols. Yang et al. [27] showed that employees' intrinsic motivation, according to SDT, fosters security-compliant behavior, albeit only regarding employees' willingness to use password managers. Li et al. [16] investigated how cybersecurity awareness, corresponding to the SDT factor *competence*, affects cybersecurity behavior. The authors demonstrate that employees who know more about the organization's security policies and procedures act more security-compliant. Conversely, Reeves et al. [19] conducted a study on negative motivators. Their results suggest that overexposure to security training or forced security procedures (such as frequent password changes) can lead to "security fatigue", leading employees to exhibit non-compliant behavior. Additionally, Goel et al. [9] researched the effect of extrinsic motivators on security compliance. The results indicate that financial rewards and punishments increase security-compliant behavior. In further user studies, Renaud and Zimmermann [20] found that nudges can enable users to choose stronger passwords, and Golla et al. [10] demonstrated that nudges can increase the use of two-factor authentication. In summary, prior research either investigated the topic from a purely theoretical viewpoint or only focused on specific motivational factors (such as employees' competence) or specific aspects of security compliance. In contrast, our study takes a broader approach, aiming to investigate how different organizations have adopted motivational strategies to foster security-compliant behavior. By comparing our findings with existing research, we contextualize our results within the broader body of knowledge, highlighting areas of agreement and identifying opportunities for organizations to refine their current 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]

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.

[1] https://github.com/employee-motivation/questionnaire
[2] The IRB certificate is available online: https://gfew.de/ethik/MwJFdwPK

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.

3.4 Coding and Analysis

To analyze the use of strategies to motivate employee motivation in cybersecurity, we used a deductive analysis approach [3] to map interview data with the theory-based classification of employee motivation introduced in Section 2. This classification served as an initial codebook. Two authors refined the coding structure through multiple rounds, resolving conflicts with flexible coding [4]. 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:

> *"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 organizations also offer annual training. Research shows that periodic training courses are critical for the cybersecurity competence of employees [11]. 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. 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 inform employees about security compliance, typically comprising password or USB stick guidelines. Employees report difficulties with those policies:

> *"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 belonging among employees. 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.

However, multiple employees reported a lack of cybersecurity relatedness in their organization. They argue that managers' commitment to cybersecurity is a prerequisite for their commitment to cybersecurity. Only if the management regards security as a central component of the business will the employees' relatedness to the organization also lead to compliance with security regulations. In short, employees want managers to lead cybersecurity by example, as one noted:

> *"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)

In sum, relatedness can foster security-compliant behavior, but often, management lacks cybersecurity commitment, diminishing employees' relatedness.

Autonomy. We found that employees' autonomy toward security-related practices is often restricted. Across the board, participants conveyed that cybersecurity training sessions are compulsory, frequently accompanied by a mandatory assessment. This obligatory nature tends to diminish participants' motivation. Most employees focused merely on completion rather than comprehension of the training. Thus, cybersecurity trainings have a negligible impact on learning:

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

The issue extends beyond training to security policies. For example, some organizations require employees to change their passwords every three months to increase security. Yet, it inadvertently promotes only a minimal adjustment of

the passwords. The coercion also leads to employees questioning the usefulness of the policies and behaving in a non-compliant manner, as one employee admitted:

> *"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, we identify a major issue: The compulsion of cybersecurity measures leads to a culture of superficial compliance. Instead of increasing security by enforcing guidelines, organizations are weakening their cybersecurity posture.

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.

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. Email programs warn employees of potential threats by highlighting emails originating from outside the organization. A security specialist explains the goal:

> *"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)

This measure increases caution by prompting employees to check emails thoroughly before interacting with their content. Yet, the lack of granularity in its application limits the effectiveness of information visibility nudges. Interviewees highlighted that emails are not categorized according to the likelihood of being phishing attempts. Instead, they are uniformly flagged when originating from external senders. 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)

In total, nudges can promote security-compliant behavior of employees, but overuse 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.

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	•	•	•	•	•

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 [17]. Organizations can emphasize that cybersecurity is a collective responsibility, as anyone could be a weak point. When management leads by committing to cybersecurity and its practices, they motivate their employees to behave security-compliantly and underscore their central role in the organization's cybersecurity efforts. By improving relatedness, cybersecurity can become part of everyone's job.

The fighter analogy by Solms et al. [22] could serve as a suitable approach to convey this responsibility to employees. Based on firefighting principles, this approach trains employees to detect and extinguish fires to protect their organization. Transferring this analogy to cybersecurity, every employee is a security fighter who can detect and fight security incidents. This analogy can be used to illustrate a culture for employees where everyone sees themselves as a contributor to ensuring the organization's security. In summary, this approach raises employee awareness and cultivates a sense of ownership and empowerment.

Organizations can leverage *messenger reputation* nudges to communicate the analogy of cybersecurity as a shared responsibility and the cybersecurity priority. Jesse and Jannach [13] describe that these nudges are effective, as employees are more willing to follow the lead of people they respect and trust. Therefore, leaders within the organization are an advantageous fit for communicating cybersecurity news and practices.

5.2 Personalized and Voluntary Education

Li et al. [16] 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]. This one-size-fits-all approach also fails to accommodate the varying levels of expertise and roles within an organization, leading to a low learning effect. By offering training tailored to the previous knowledge and specific requirements of employees, organizations can ensure that the learning material is relevant and accessible. This increases knowledge retention and highlights the applicability of the training to employees' daily tasks. Driven by the enhanced learning experience, the workforce is thus more competent and motivated to adopt security-compliant behaviors.

Fisher [6] suggests offering voluntary education programs instead of forcing employees. Despite the clear advantages, no interviewees' organization offers voluntary learning opportunities. Employees eager to expand their knowledge or specialize further in certain cybersecurity areas often find themselves unable to do so. Organizations can address this gap by offering voluntary training courses that empower employees to extend their learning journey, pursuing further education out of genuine interest rather than obligatory compliance. This autonomy in learning fosters intrinsic motivation, which is known to substantially enhance the effectiveness and depth of the learning experience [24].

Generative AI (GenAI) emerges as a solution for organizations to offer personalized and voluntary training. While some organizations have customized training for specific departments, GenAI's capabilities extend personalization to an individual level, adapting the content and extent of training to meet each employee's unique background and needs. This level of customization ensures that training is more engaging and compelling, tailored to each learner. Put simply, by integrating GenAI into their cybersecurity training, organizations can promote their employees' competence and motivation for 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. [19] suggest moving away from outdated protocols like mandatory periodic password changes to more effective and user-friendly measures. Thus, organizations can foster employee commitment to cybersecurity by preserving employees' autonomy. Additionally, Fisher et al. [6] 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 [20] and Golla et al. [10]. 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

Organizations can use employee-generated security reports to enhance their cybersecurity posture. By acknowledging and utilizing these security reports, organizations can increase a sense of relatedness and contribution among employees. Thus, employees can perceive the impact of their efforts and experience autonomy by feeling empowered. This recognition can be a powerful motivator, encouraging employees to continue reporting and adopting security-compliant behavior. Moreover, timely and constructive feedback on these reports can enhance the competence of employees. As they learn to identify and understand threats, employees can improve the quality of the reports and better protect themselves and the organizations from security incidents.

Adopting a healthy error culture within the organization is crucial to motivating employees toward security-compliant behavior. While Goel et al. [9] 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, but their success requires careful application. Overuse can lead to security fatigue, reduce effectiveness, or even undermine desired behavior. Thus, organizations should adopt a more nuanced approach, like refining email warnings to provide more specific and relevant alerts. With a targeted strategy, nudges can unfold their potential and increase 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. 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)
4. 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)
5. 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)
6. 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)
7. Gagné, M., Deci, E.L.: Self-determination theory and work motivation. Journal of Organizational behavior **26**(4), 331–362 (2005)
8. 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)
9. 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)
10. 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)

[3] We outline AI Usage Cards [26]: https://ai.uversy.com/employee-motivation

11. 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)
12. 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)
13. Jesse, M., Jannach, D.: Digital nudging with recommender systems: Survey and future directions. Computers in Human Behavior Reports **3**, 100052 (2021)
14. 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)
15. Leonard, T.C., Thaler, R.H., Sunstein, C.R.: Nudge: Improving decisions about health, wealth, and happiness. Constitutional Political Economy **19**(4), 356–360 (12 2008)
16. 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)
17. 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)
18. 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)
19. Reeves, A., Delfabbro, P., Calic, D.: Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. SAGE open **11**(1) (2021)
20. Renaud, K., Zimmermann, V.: Nudging folks towards stronger password choices: providing certainty is the key. Behavioural Public Policy **3**(2), 228–258 (2019)
21. 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)
22. 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)
23. Statista: Estimated cost of cybercrime worldwide 2017-2028 (11 2023), https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide, accessed: 01/08/24
24. 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)
25. Verizon: 2023 data breach investigations report. Tech. rep. (2023)
26. 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)
27. 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)