Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory

Muriel Frank[a,b,*], Vanessa Kohn[a]

[a] Goethe University Frankfurt, Frankfurt, Germany
[b] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

ARTICLE INFO

Article history:
Received 2 May 2023
Revised 29 June 2023
Accepted 6 July 2023
Available online 8 July 2023

Keywords:
Behavioral information security
In-role behavior
Extra-role behavior
Organizational citizenship behavior
Self-determination theory
Construal level theory
Psychological distance

ABSTRACT

Extra-role security behaviors (ERSBs) – spontaneous security behaviors that are not prescribed in organizational security policies – are seen as a useful addition to securing informational assets in organizations. However, this exploratory study, based on findings obtained through 29 in-depth-interviews, challenges this positive perspective and shows that extra-role security behaviors cut both ways: They are either helpful or harmful. In addition, our results suggest that (1) ERSB contributes to varying degrees to the effectiveness of information security compliance, (2) the self-determination theory contributes to understanding the motivators for ERSB, and (3) the construal level theory of psychological distance explains the differential risk evaluation of ERSB. We discuss implications for researchers and practitioners – particularly in terms of promoting the beneficial nature of extra-role security behaviors – and suggest compelling avenues for future research.

1. Introduction

Implementing information security policies (ISP) is one of the standard repertoires of contemporary organizations. ISPs specify how information technology users should behave in order to safeguard organizational assets from potential security breaches (Bulgurcu et al., 2010). In particular, ISPs provide instructions on how to avoid, detect, or respond to information security incidents (Cram et al., 2017). Over the past decade, scholars have repeatedly emphasized the importance of individuals' ISP compliance when aiming to increase policy effectiveness and combat security threats (Hsu et al., 2015), with reviews on the taxonomy (Guo, 2013; Padayachee, 2012), its theoretical underpinnings (Lebek et al., 2014), and its antecedents (Cram et al., 2019; Sommestad et al., 2014).

In recent years, however, research has shown that relying on individuals only to comply with security policies and regulations is no longer sufficient (Hsu et al., 2015; Jaeger and Eckhardt, 2018), as these policies cannot cover all (un)desirable security behaviors nor all emerging security incidents and threats (Chen and Li, 2019; Hsu et al., 2015). Therefore, to protect information resources, extra-role security behaviors (ERSB) are required – discretionary security behaviors that are not specified in the ISP nor elicited by punishment or reward (Hsu et al., 2015). These behaviors can come in the form of helping others with security-related issues (helping), bringing new threats to others attentions (voicing), reporting malbehavior (whistleblowing) or cautioning colleagues about security threats (stewardship) (Frank and Ranft, 2021; Hsu et al., 2015; Jaeger and Eckhardt, 2018; Nehme and Marler, 2023). First empirical investigations show that extra-role security behaviors positively influence employees' policy compliance (Li et al., 2017) and ISP effectiveness (Hsu et al., 2015). Thus, we see important differences between these forms, but we still lack a comprehensive understanding of extra-role behaviors, as we see in other research areas (see e.g. Podsakoff et al. (2000)). Consequently, we see the need to identify, describe, and classify discretionary security behaviors prevalent in contemporary organizations and to substantiate them with concrete examples in order to answer our first research question, which is as follows:

What types of extra-role security behaviors are prevalent in modern organizations?

Because of their importance for security compliance and to prevent security incident (Nehme and Marler, 2023), researchers recently started to examine factors that motivate or prevent engagement in extra-role security behaviors (e.g., Chen and Li 2019, Frank and Ranft 2021, Guan and Hsu 2022, Nehme and Marler 2023, Ogbanufe and Ge 2023). However, research is still scarce and scattered. So far, just a dozen studies explicitely deal with moti-

[*] Corresponding author at: Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg.

E-mail address: muriel.frank@uni.lu (M. Frank).

https://doi.org/10.1016/j.cose.2023.103386

vation for extra-role security behaviors. Building on the person-organization fit theory, Chen and Li (2019), for instance, find that apathy reduces the intention to perform extra-role security behaviors while security commitment increases engagement in extra-role security behaviors. With the help of 78 IS managers and 260 employees in Taiwan and building on the social control theory, Hsu et al. (2015) demonstrate that social control, such as commitment or attachment, increases the possibility of prosocial behaviors. Ogbanufe and Ge (2023) reveal that your role identity has a substantial influence on whether employees take actions to protect their organization's security. Using machine learning techniques, Frank and Ranft (2021) show that informational, social and task context factors impact the likelihood of reporting suspicious e-mails to the IT helpdesk. It seems that motivators differentiate employees who perform extra-role security behaviors from those who are not willing to engage in extra-role behaviors. Yet, research lack insights into how these motivators differ for various types of ERSB. Hence, the second question we address is as follows:

How do people differ in their motivation to engage in extra-role security behaviors?

Building on the self-determination theory (SDT) (Deci and Ryan, 1985), which has been successfully applied in the information security field before (e.g., Padayachee 2012), the present study aims to decode the motivational factors that influence extra-role security behaviors, i.e., it classifies extra-role security behaviors in a new taxonomy to understand what needs or motives are met by such proactive behaviors. In this way, our research will provide new insights that will help managers and researchers better understand individuals' security behaviors and encourage behaviors that contribute to an organization's information security. This seems especially vital as previous research has shown that extra-role security behaviors can boost information security policy compliance (Jaeger and Eckhardt, 2018) and prevent security incidents (Nehme and Marler, 2023). In addition, understanding people's motivation for engaging in extra-role security behaviors allows for more targeted approaches to encourage their willingness to go the extra-mile for information security and thus voluntarily go beyond their prescribed in-role activities.

The paper is organized as follows. The next chapter briefly reviews the relevant literature on extra-role security behaviors, highlighting the research gap and unique contribution of our work. It also introduces the methodological procedures of data collection and data analysis. In the third chapter, nine dimensions of extra-role security behaviors are identified and exemplified in line with the first research question. The fourth chapter introduces self-determination theory, which serves as a theoretical basis for understanding the factors that influence engagement in extra-role security behaviors. Next, it arranges extra-role security behaviors as a taxonomy based on self-determination theory to answer the second research question. During data analysis, we discovered a double-edge sword effect of extra-role security behaviors, which we present and explain in the fifth chapter drawing on the construal level theory of psychological distance. Finally, we discuss limitations and future research opportunities related to our work.

2. Theoretical background and methodological procedure

2.1. State of the art: extra-role security behaviors

Most conceptualizations of organizational behavior suggest that it has two dimensions: in-role behaviors, which refer to behaviors that are formalized contingent on a given role or job position, and enforced or rewarded by leadership (Van Dyne et al., 1995; Katz, 1964), and extra-role behaviors – prosocial behaviors that go beyond prescribed and expected work activities, intend to benefit the employer and are essential to the effective functioning of an organization (Van Dyne et al., 1995; Katz, 1964; Organ, 1997). Extra-role behaviors are also referred to as organizational citizenship behavior (Van Dyne et al., 1995).

Although researchers began studying extra-role behaviors as early as the 1930s, it was not until after the studies by Organ and his colleagues (see, for instance, Smith et al. 1983) that this topic gained much attention (LePine et al., 2002). Since then, research on extra-role behavior has expanded from the field of organizational behavior to other disciplines, such as human resource management (e.g., Newman et al. 2016), marketing (e.g., Podsakoff and MacKenzie 1994), management (e.g., Morrison 1994), and psychology (e.g., LePine et al. 2002). However, the rapid growth in empirical research has produced various forms of extra-role behavior, which according to Podsakoff et al. (2000) can be synthesized into seven main dimensions: (1) helping behavior, (2) sportsmanship, (3) organizational loyalty, (4) organizational compliance, (5) individual initiative, (6) civic virtue, and (7) self-development.

In the information security domain, behaviors associated with or defined in organizational information security policies are usually referred to as in-role activities (Chen and Li, 2019). Such behaviors, for example, range from guidelines for secure password management to access management regulations and security handbooks. In contrast, extra-role security behaviors encompass spontaneous security actions that are not defined by organizational rules or policies (Hsu et al., 2015). Examples include implementing a new idea that helps improving information security policies and addressing security incidents (Guan and Hsu, 2022) as well as reporting colleagues' security wrongdoings to supervisors and offering assistance on security topics (Jaeger and Eckhardt, 2018).

Compared to the large number of research studies addressing in-role behavior (e.g., Cram et al. 2019, D'Arcy and Lowry 2019), few researchers have addressed extra-role security behavior. Among the first were Hsu et al. (2015) who examined the impact of extra-role behaviors on information security policy effectiveness as well as the impact of formal and social controls on those behaviors. Their findings show that employees are more likely to perform extra-role security behaviors if they feel connected to peers or share the same norms and values. Three years later, Jaeger and Eckhardt (2018) built on the work of Hsu et al. (2015) and shed light on the role of information security awareness on extra-role security behavior. Their findings suggest that employees with security awareness are more likely to help and speak up, while employees with policy awareness are more likely to report wrongdoing and engage in stewardship. More recently, Ogbanufe and Ge (2023) brought identity theory into play and demonstrated that engagement in extra-role security behaviors – measured as in Hsu et al. (2015) – is influenced by whether people feel that information security is part of their role identity. Drawing on social control theory, Wang et al. (2022) show that extra-role behavior is mediated by security policy compliance and peer behavior.

Other authors like Li et al. (2017), Guan and Hsu (2022) and Nehme and Marler (2023) propose frameworks that explore the antecedents of and motivators for extra-role security behavior, but empirical validation is lacking. Research by Guhr et al. (2019) illustrate that transformational leadership promotes prosocial behaviors such as intention to participate in security. Chen and Li (2019) provide evidence that fit elements establish security commitment and performance of extra-role security behavior. More recently, Hu et al. (2021) have shown that positive attitudes towards security programs increases the likelihood of performing extra-role security behavior, and Frank and Ranft (2021) explore the contextual determinants of prosocial behaviors, in particular reporting malicious e-mails.

In summary, the majority of research conducted to date has primarily illuminated the positive aspects of extra-role security behavior, such as improved policy effectiveness (Hsu et al., 2015) or

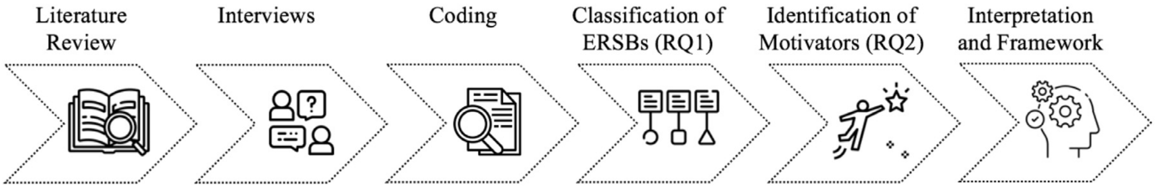
Literature Review
Interviews
Coding
Classification of ERSBs (RQ1)
Identification of Motivators (RQ2)
Interpretation and Framework

Fig. 1. Structure.

boosted security commitment (Chen and Li, 2019). The exception is a study by Jia and Xu (2021), which for the first time also addresses negative aspects of extra-role security behavior. The authors examine the conditions under which extra-role security behavior leads to security carelessness or misuse of resources. That being said, research examining different types of extra-role behavior seems to be rather selective; most scholars focus on helping (Hsu et al., 2015), stewardship, or whistleblowing (Jaeger and Eckhardt, 2018), which leaves room for further investigation. Consequently, we see the need to systematically study these behaviors.

2.2. Methodological approach

2.2.1. Procedure

In order to identify and classify prevalent extra-role security behaviors and further identify the motivational factors that explain why people engage in prosocial behaviors, this study draws on data collected in 29 in-depth semi-structured interviews with German professionals. Fig. 1 illustrates our procedure, which is broken down into all the steps necessary to answer our two research questions. All participants volunteered to be interviewed following our outreach. We targeted IT professionals as well as non-IT professionals, as it is encouraged to include both when studying security-related behaviors (Hsu et al., 2015). To minimise response bias (Podsakoff et al., 2003), we assured each respondent of confidentiality and anonymity. Among the interviewed professionals, the majority work in positions without managerial responsibilities (72.41%), and only 27.59% hold managerial positions. On average, they were 37.76 years old with a standard deviation of 11.34 and had 15.24 years of work experience.

Since the goal of this exploratory study is to understand what drives employees to engage in or refrain from performing different types of extra-role security behaviors, we conducted semi-structured interviews. By doing so, we were able to ask questions in a conversational style so that the discussion evolved based on respondents' prior answers. This allows for a deeper understanding of complex perceptions and motivations around extra-role behaviors, while maintaining high reliability and validity (Barriball and While, 1994). As the distinction between in- and extra-role behaviors is contingent (Vey and Campbell, 2004), we refrained from using these terms in our interviews to not influence respondents' answers. The complete interview protocol can be found in Appendix A.

In the beginning of each interview, questions centered around the respondent's general perception of IT security and their role. We also wanted to learn more about their knowledge of organizational practices and measures to improve IT security and whether they are interested or involved in them. In the second part of the interview, we explored their actual extra-role security behaviors. For example, we asked them "Have you ever engaged in behaviors that go beyond your information security obligations?" If they answered "yes", we also inquired about their motivations. We also asked if they have ever witnessed colleagues circumventing security guidelines. If so, we wanted to know how they dealt with it and what motivated them to do so. Otherwise, we described two scenarios to capture respondents' intentions regarding extra-role security behaviour. Using scenarios to investigate individuals behaviors is a common method in information security (D'Arcy et al., 2009). The first is a scenario in which a colleague forgets to lock their screen when they leave the desk. The second one describes a scenario in which a colleague receives a customer request that violates the company's security policy. In both cases, we asked respondents what they would do and why. In the final block, we were interested about respondents' organizational cultures, especially with regard to error tolerance, and whether they feel encouraged to help colleagues with IT security-related issues or to share security-related experiences.

All 29 interviews were digitally recorded and transcribed with the participants' consent. They comprise a total of 93.783 words and build the empirical foundation of this study.

2.2.2. Coding and assessment

The goal of our data analysis is two-fold: first, to identify specific extra-role security behaviors that are prevalent in modern organizations and classify them into higher-level categories (see Chapter 3), and second, we aim to decode the motivators and demotivators for the identified extra-role security behaviors (see Chapter 4.2). We followed the guidelines for the analysis of qualitative data by Klein and Myers (1999) and Walsham (2006). Coding, which included multiple cycles, was based on Saldaña (2013).

With regard to the first research question, two researchers independently examined the transcripts for all mentions of extra-role security behaviors. Joint analysis of interviews with more than one coder is common in scientific research (see, for example, Castilla and Ranganathan 2020, Kelle 1995). During the first coding cycle, the researchers identified more than 100 statements with regard to various extra-role security behaviors and more than 40 specific examples. In a second step, the researchers used elaborative coding to combine similar examples identified in the interview transcripts into nine major dimensions of extra-role security behavior found in the literature (Van Dyne et al., 1994; Podsakoff et al., 2000). In 84.38% of all cases, both coders agreed with their categorization of particular extra-role security behaviors to particular extra-role security behavior dimensions, which is within the accepted intercoder agreement of 80% to 90% (Saldaña, 2013). For those examples where there was disagreement, the coders engaged in an in-depth discussion and also included expert opinion and related research, which ultimately led to a consensus assignment of all examples to the categories of extra-role security behavior.

To identify motivational cues in the data, two researchers first examined the transcripts for positive and negative statements about extra-role security behaviors. They identified and coded more than 130 statements containing motivational information. The coders then shared their coding schemes captured in their codebooks to clarify the properties of the codes. In a subsequent cycle, they thematically organized the underlying motivational cues – positive statements containing motivating and negative statements demotivating factors – into higher-level categories of motivators and demotivators. Following Harry et al. (2015), the two researchers compared their coding of the data to develop consistency in the use of the codes and in this way increase reliability.

The aligned list of motivational cues was used in a final step to align the identified motivators along a continuum from extrinsic to intrinsic motivation (see Chapter 4.2).

3. Categorization of extra-role security behaviors

As extra-role behaviors have been largely overlooked in the security context (Hsu et al., 2015), the first objective of this study is to identify the types of extra-role behavior that play a significant role in the information security domain. To do so, we build on prior research in the organizational domain, particularly on Podsakoff et al.*'s* (2000) classification of organizational citizenship behavior and Van Dyne et al.*'s* (1995) nomological network for extra-role behaviors. Van Dyne et al. (1995) typology of extra-role behaviors consists of four distinct dimensions: helping (=voluntary actions aimed at supporting others), voice (=challenging the behavior of others to improve a situation), whistleblowing (=reporting the misconduct of others to effect change) and stewardship (=intervening in behaviors to protect others). Podsakoff et al. (2000) share the helping dimension with Van Dyne et al. (1995) but identify six additional dimensions. Among them are sportsmanship (=accepting adversity without complaining), organizational loyalty (=defending the organization against threats), organizational compliance (=remaining compliant even when no one is watching), individual initiative (=voluntarily doing more than required to improve performance), civic virtue (=constructive involvement in procedures aimed at protecting the organization) and self-development (voluntarily improving skills).

To verify whether and how these dimensions are also specific to the information security context, we conducted 29 interviews with employees who are confronted with security policies and regulations in their daily work. During the interviews, all participants were asked to provide examples of prosocial behaviors, thus describing whether and how they went above and beyond what was required or mandated by information security policies and regulations. As a result of the interviews and the literature review, we identified nine dimensions of extra-role security behaviors (see Tables 1 and 2). Below we will describe each of the nine ERSB dimensions and illustrate them with examples from our interview data.

Helping. The most frequently mentioned dimension of extra-role security behavior is helping. Interview responses indicate that employees voluntarily help coworkers with security-related problems, share their information security knowledge, or give them advice on how to act more securely in their day-to-day work. It can be seen as proactive assistance which fosters collaboration among peers (Van Dyne and LePine, 1998; Li et al., 2021). In many cases, it is altruism, meaning that people perceive the act of helping as enjoyable and interesting (*"If a colleague approaches me with a security problem and I can solve it, I am helper number 1.", P13; "I am happy to share my knowledge.", P09).* Interestingly, respondents also point to potentially negative outcomes of extra-role security behavior – a view that has been largely neglected in the context of extra-role security behavior (Guan and Hsu, 2022). They report that extra-role behavior can lead to security policy violations, such as sharing wrong information and giving wrong advice. A 55-year-old clerk therefore stated that she would advise others to contact appropriate professionals for IT security issues rather than trying to help on their own.

Stewardship. Interviewees also referred to behaviors transcribed as stewardship, i.e., when more skilled workers help others with the intent to protect them from harm (Van Dyne et al., 1995; Jaeger and Eckhardt, 2018; Li et al., 2021). For instance, they actively intervene when coworkers engage in risky security behaviors, such as failing to lock their computer screen when leaving the work area, writing down their passwords and leaving them in plain sight, or leaving customer data exposed on the table. The reason why employees provide this kind of constraints is not only to prevent their colleagues from causing a security breach but also to prevent them from facing professional disadvantages, like receiving a note for the file (*"Sometimes you see that they have pieces of paper with all the passwords on them. So, of course, you tell them that is not a good idea because I want them to be safe.", P13).*

Sportsmanship. During the interviews, participants reported their tolerance of information security inconveniences at work. As stated by prior research, information security policies and requirements can disrupt employees' work tasks, are sometimes difficult to understand, and pressure employees (Ament and Haag, 2016; D'Arcy et al., 2014). Interview respondents also confirm that information security implies extra effort and time (*"For me, IT security primarily means restrictions.", P05).* However, these inconveniences associated with securing information assets in the workplace are unavoidable. Sportsmanship in the information security context means that employees accept these obstacles without complaining. They acknowledge that information security is time-consuming, but they still follow the rules rather than taking shortcuts or violating policies.

Organizational loyalty. Evolves around behaviors like staying committed even during hard times, i.e., in the case of security incidents, and spreading goodwill. For instance, interviewees call for conditions that improve employee behavior related to information security because they want the company's reputation to be enhanced. Furthermore, interview participants mentioned that they promote their companies' values and security-related procedures to outsiders. Organizational loyalty also means protecting an organization from threats, e.g., refusing to circumvent established security measures in the event of a potential breach, but proposing a policy-compliant alternative. (*"When someone asks me to violate a security directive, I look for a solution that complies with the policy.", P16).* Respondents also show loyalty to their employer by taking precautions either to prevent espionage and data theft *("I proactively intervene […] to protect the company and the stakeholder involved from security issues.", P14).*

Organizational compliance. Represents impersonal behaviors reflecting a person's compliance with norms, rules, regulations, and policies. Employees also adhere to exactly these rules if no one is overseeing their actions. That involves a high degree of internalization of a companies' rules and regulations. Being compliant does not help the individual but rather the whole organization. Being compliant involves following security-related rules and knowing where to look up the security policies when needed *("I care about security policies or policies in general, I accept them, I abide by them, and by doing so I want to show that these internal processes are important to me."* (P17). In the information security context, policy compliance is often considered in-role behavior as everyone is expected to always adhere to these policies (Jaeger and Eckhardt, 2018). However, this is not the case for many employees, which has been confirmed in various empirical studies (Cram et al., 2017, 2019). Our interviews reveal a similar picture. Respondents admit to being comfortable with bypassing established security measures when they are in a hurry. Hence, in our study we consider information security compliance an extra-role security behavior.

Civic virtue. While prior research interprets civic virtue as being actively engaged in the organization's governance (George and Brief, 1992; Podsakoff and MacKenzie, 1994), we find that civic virtue in the context of information security does not fit the definition. Instead, in the information security context, civic virtue comprises active participation in information security processes, procedures and measures with the intent to improve their organization's overall information security. This, for instance, includes challenging others behavior with the intention to improve ways of execut-

Table 1
Dimensions of extra-role security behavior - Part 1.

	General definition	Security-related definition	Examples (from the interviews)	Challenges
Helping	Refers to voluntary acts granted to others when the occasion calls it, such as helping with work-related problems (Smith et al., 1983), supporting career starters even though it is not required (LePine et al., 2002), or training others on new tasks or equipment (Wollan et al., 2009)	Entails behaviors of helping coworkers with security-related issues and tasks.	• Helping colleagues with security-related questions • Sharing security knowledge • Sharing advice concerning passwords, phishing e-mails	Employees could share erroneous information and give wrong advice which might be harmful to the organization.
Stewardship	Refers to the behavior of more experienced and powerful employees who prevent their colleagues from performing a harmful or illicit act in order to protect them (Van Dyne et al., 1995)	Prohibiting or restricting behaviors of less security-aware employees to protect them from security incidents or violations of security policies	• Prohibiting coworkers from taking sensitive documents home • Preventing peer from not locking their computer screen when leaving the workplace	
Sportsmanship	Includes behaviors aimed at tolerating less than ideal circumstances without complaining, avoiding railing against real or imagined offenses, or making problems bigger than they are (Moorman, 1993; Podsakoff and MacKenzie, 1994)	Involves tolerating security-related work impediments without complaining about them.	• Tolerating the extra time needed to fulfill security policies without complaining	Accepting impediments without complaining might prevent employees from suggesting improvements to the respective processes (see civic virtue).
Organizational loyalty	Comprises prosocial behaviors directed toward the organization (Rioux and Penner, 2001)	Includes spreading goodwill, protecting the organization from and remaining committed during data breaches.	• Promoting security regulations to outsiders	Might misrepresent the organization.
Organizational compliance	Evolves around when workers have internalized their organization's values, rules, and procedures, which results in adherence to them even when no one is around to monitor their compliance (Podsakoff et al., 2000; Smith et al., 1983)	Refers to adherence to security-related norms, rules, and procedures.	• Adhering to the information security policies • Internalize security-related norms	

ing security in their organization or reporting suspicious activities *("When I receive suspicious emails, I forward them to the IT department.", P27)*. Overall, employees recognize that they are a member of a larger whole and accept the responsibilities of being part of an organization (Podsakoff et al., 2000). They seem to understand that they have a stake in securing their company. Our interview partners, for instance, reported that they proposed adjustments to security procedures.

Individual initiative. Employees who show this kind of extra-role security behavior go well beyond what is minimally required. They voluntarily change their passwords or choose longer passwords even when this is not expected, they use privacy filters for computer screens and voluntarily take on additional responsibilities, such as informing colleagues about how to behave more securely in their private environment. Employees also report that their colleagues voluntarily organize meetings to discuss security-related issues. In order to increase organizational security, employees also adopt additional security measures when setting up virtual private networks, or they turn on flight mode when they are not actively using their cell phones *("I voluntarily change my password regularly, even if it is not required, because I know that anything else is a security risk.", P17)*. Our interviews also indicate that some employees are overzealous when it comes to their company's security, resulting in security policy violations. For example, one interviewee reported that he rolled back an update because he felt it had security vulnerabilities.

Whistleblowing. Another prosocial behavior is whistleblowing, which is about reporting wrongdoings or illegitimate acts (Van Dyne et al., 1995). Employees do not only disagree about their colleagues' behavior but disclose their misdemeanors to a higher authority *("If we find that an employee has unapproved software on his or her computer, […] this may result in the supervisor also being informed, if necessary." (P11)*. However, not all respondents favor this whistleblowing strategy, as they do not want to contribute to the pillorying of the guilty *("I wouldn't denounce my colleagues.", P26)*. One interview participant reported that she would be more likely to report her peers if the goal was not to find someone to blame, but to solve problems and avoid mistakes in the future.

Self-development. Another form of extra-role security behavior is self-development. Employees are willing to acquire new security knowledge. In order to keep up with the constant changes in security requirements and technological changes, employees dedicate parts of their free time to extending their knowledge in the field of information security. Interview partners mentioned listening to podcasts or watching YouTube tutorials on security topics. Self-development may also encompass attending non-compulsory training sessions and information security lectures at the university *(„I voluntarily educate myself in security topics because it is of interest to me and I want to acquire knowledge.", P21; "I like to listen to podcasts on this topic because it interests me.", P10)*.

Table 2
Dimensions of extra-role security behavior - Part 2.

	General definition	Security-related definition	Examples (from the interviews)	Challenges
Individual initiative	Range from communicating with peers in order to boost group performance (Moorman and Blakely, 1995), making constructive suggestions for improvement (George and Brief, 1992), and offering to take on extra responsibilities (Podsakoff et al., 2000).	Encompasses behavior that goes well beyond what is required, i.e., take on responsibilities associated with information security.	• Using longer passwords than required • Changing passwords regularly even if not required • Refraining from cyber loafing on a work computer • Restarting work computer between two presentations to make sure that no sensitive data is visible • Locking the computer screen when leaving the workplace • Refraining from using private USB sticks • Using VPN for more security • Encrypting PDFs • Checking if one's e-mail address has been hacked	Employees opt for security measures that have not been approved by their organization, e.g., they remove an update because they consider it insecure
Civic virtue	Includes challenging behavior in order to improve a particular situation (Van Dyne et al., 1995)	Refers to active organizational participation, including voicing improvements concerning information security procedures and measures	• Submitting improvements concerning information security via ticket system • Advising colleagues not to use external USB sticks	
Whistleblowing	Disclosure of illicit activities and wrongdoings to management in order to effect change (Van Dyne et al., 1995)	Refers to confronting illicit security activities of colleagues and reporting them to supervisors or managers to effect change.	• Reporting someone who is poses a great security risk • Reporting when colleagues exchange passwords with each other • Reporting of colleagues circumventing security policies	Disclosing illicit activities of colleagues might cause challenges for the working atmosphere.
Self-development	Consists of workers who seek to improve their skills and knowledge to do their jobs better or to acquire better positions in the organizations (George and Brief, 1992)	Involves a need for enhancing one's security skills and knowledge.	• Listening to security podcasts • Watching YouTube tutorials • Attending non-mandatory security training sessions • Attending lectures about information security	mployees could obtain information from non-legitimate sites and base their decision on incorrect information.

Addressing the first research question, extra-role security behaviors can be categorized into nine dimensions, ranging inter alia from helping to sportsmanship and individual initiative to self-development. Based on the results of our interviews, and contrary to the understanding of most scholars (e.g., Cram et al. 2017), organizational compliance behavior is considered as extra-role security behavior. This is because following rules, even when no one is watching, is a voluntary behavior that is not triggered by either rewards or punishments and thus meets the definition of extra-role security behavior. Surprisingly, some of the dimensions cut both ways, i.e., they can be either beneficial or detrimental to an organization's security goals. We call this the double-edged sword effect of ERSB. In Chapter 5, we will elaborate on this phenomenon in greater detail.

4. Integration of self-determination theory

4.1. Introduction to self-determination theory

Deci and Ryan's (1985) self-determination theory (SDT) postulates that human behavior can be either intrinsically or extrinsically motivated. Consequently, SDT is one of the most powerful behavioral theories in psychology and has attracted much attention in various disciplines, including the field of information security (Padayachee, 2012). In the working context, SDT posits a descriptive continuum, thereby acknowledging the interconnection of extrinsic and intrinsic motivation (Gagné and Deci, 2005). On the one end, there is intrinsic motivation, which assumes that the individual performs an activity for its own sake (Deci, 1971), because it is enjoyable or interesting (Visser, 2017). On the other end is amotivation, which means the absence of any motivation (Vallerand, 1997). And in-between, the continuum shows different types of extrinsic motivation – external reasons for showing behavior – which vary in their degree of self-determination (Gagné and Deci, 2005). An overview of the motivation continuum is presented in Fig. 2.

The self-determination continuum does not represent a stage theory but rather describes to which extent individuals have internalized behaviors (Gagné and Deci, 2005). Intrinsic motivation deals with behavior that are performed in the absence of incentives because it is inherently enjoyable and interesting (Deci and Ryan, 1985). Intrinsically motivated behavior is inherently autonomous meaning that individuals perform activities without feeling compelled to do so (Gagné and Deci, 2005). Such behavior is accompanied by a sense of competence, which means that the individual perceives the activities as being performed effectively (Niemiec and Ryan, 2009).

If activities are not interesting or enjoyable, extrinsic motivation, such as rewards, is required. Extrinsic motivation, however, varies in the degree of autonomy respectively self-determination, hence the perception of acting of their own volition and having the choice (Deci and Ryan, 1987; Gagné and Deci, 2005).

SDT postulates four different manifestations of extrinsic motivation: controlled motivation, moderately controlled motivation, moderately autonomous motivation to autonomous motivation. Controlled motivation refers to extrinsic behavior that is accompanied by pressure and anxiety (Deci and Ryan, 1987). When controlled motivated, individuals act with the intention to avoid an unpleasant outcome or achieve a desired outcome (Gagné and Deci, 2005).

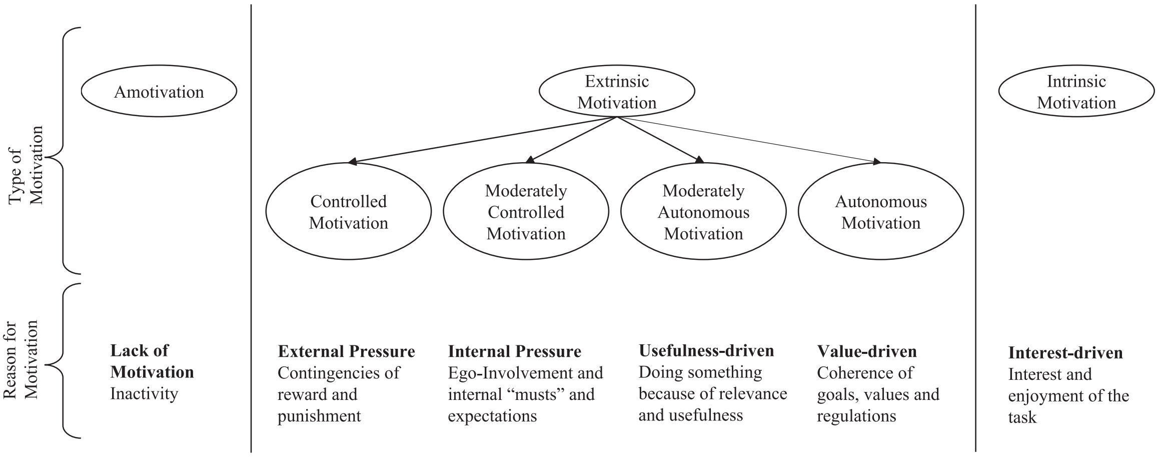
Type of Motivation
Amotivation
Extrinsic Motivation
Intrinsic Motivation
Controlled Motivation
Moderately Controlled Motivation
Moderately Autonomous Motivation
Autonomous Motivation
Reason for Motivation
Lack of Motivation
Inactivity
External Pressure
Contingencies of reward and punishment
Internal Pressure
Ego-Involvement and internal "musts" and expectations
Usefulness-driven
Doing something because of relevance and usefulness
Value-driven
Coherence of goals, values and regulations
Interest-driven
Interest and enjoyment of the task

Fig. 2. The self-determination/motivation continuum by Gagné and Deci (2005) and Visser (2017).

As internalization increases, extrinsically motivated behavior becomes more autonomous. For instance, moderately controlled motivation means that individuals have internalized a particular behavior but have not accepted it as their own, e.g., people work in order to feel worthy (Gagné and Deci, 2005). People do things to live up to their own expectations (Visser, 2017). Being autonomously motivated means that one willingly and voluntarily pursues some extrinsic end (Deci and Ryan, 1987).

Moderately autonomous motivation means one feels relatively autonomous in performing unpleasant and uninteresting activities because they are consistent with personal goals and values. The activities are relevant and useful for the performer (Visser, 2017). An example of this is when nurses who care about the health of their patients bathe them, even though they find this activity uninteresting. However, when individuals are fully autonomously motivated, they perceive a particular activity as part of their identity. It is noteworthy that this type of extrinsic motivation cannot be compared to intrinsic motivation because the activity in this instance serves as an instrument to achieve personal goals and is not inherently enjoyable (Gagné and Deci, 2005).

4.2. A self-determination theory perspective on ERSB motivation

4.2.1. The continuum of extra-role security behaviors

The analysis of interview data revealed various motivational cues for engaging in ERSB. Our goal is to understand what drives employees to perform ERSB in line with the nine types characterized in the previous chapter. Drawing on the self determination theory (SDT), we aligned the identified motivators along a continuum of extrinsic to intrinsic motivation. By matching the nine ERSB dimensions to the appropriate motivational category, we learn what stimulates each ERSB type (see Table 3). This taxonomy is an essential step in supporting organizations' decision-making process on whether or not to implement measures to increase employee ERSB. In addition, it provides an understanding of which motivators are associated with potentially harmful ERSB, as the ambiguity of ERSB mentioned in the previous chapter requires a distinction to be made.

The first category of the SDT continuum reflects the lowest type of involvement – amotivation (Vallerand, 1997). It describes the feeling of being unable and unwilling to engage in any security-related action. The reasons for lack of motivation range from lack of time or disinterest to lack of ideas and laziness (e.g., *"I am too lazy to use a password manager", P16; "I don't see the benefit of doing more than is required by IT policy because I don't see the risk because misuse cases don't happen often.", P26*). Our respondents also reported that they do not intend to get involved in information security due to a lack of expertise and skills and therefore fear of spreading false information (e.g., *"I do not get involved in IT issues because I don't have sufficient knowledge.", P03*). Such observations are usually explained by social cognitive theory, which states that people evaluate their behavior over the anticipated positive and negative consequences of that behaviors and usually refrain from taking security measures, such as reporting spear-phishing emails, which could cause embarrassment, shame, or redicule if reported incorrectly (Kwak et al., 2020). Others feel they could contribute, but do not want to take on any tasks outside their scope of responsibility or are convinced that it is inefficient to voluntarily complete tasks that have not been agreed upon ("*Without a clear mandate and clear coordination and delineation of who contributes what part, I would not agree to do more so that the work is not being done twice.", P18*). This is consistent with previous research showing that users perceive information security as secondary to their daily workload (Pham et al., 2017). Often a shift of responsibility takes place when employees are convinced that automatic mechanisms are in place to sufficiently protect the organization's IT security and that only the experts are responsible for IT security. These demotivators are less interesting for our analysis, as they do not translate into ERSB. However, organizations should strive to understand why their employees refrain from performing ERSB as some of these demotivators can be countered.

Extrinsic motivation to perform ERSB ("mustification") is further distinguished into two categories (Chen et al., 2015; Visser, 2017). In the first category, motivation stems from external pressure and the need to comply with existing information security policies. Actions taken for the sake of **obedience** typically fall under the ERSB type of organizational compliance. Research on **threats** of punishment and fear appeals helps to understand why employees are motivated to engage in behaviors that are beneficial to information security (Kim et al., 2020; Orazi et al., 2019). If employees perceive a high risk of punishment, they are less likely to violate policies (Kim et al., 2020). Rewards such as a **higher salary** or a **promotion** drive some employees to perform other ERSB because it outweighs the associated costs of doing so (*"A better position, a promotion, a raise would be a condition that would have to be in place for me to do that [an.: involvement in ERSB] more.", P21*). However, some researchers argue that intrinsic motivation works better than extrinsic motivation to achieve ERSB (Frank and Ament, 2021). This is consistent with the results of our interviews which show that respondents are often not intrigued by extrinsic incentives (*"Financial incentives don't work at all to get me to engage in spontaneous behaviors.", P16*).

Table 3
Taxonomy of motivation continuum of extra-role security behaviors.

	Amotivation			Extrinsic motivation		Intrinsic motivation
Reason for ERSB	No intention	External pressure	Internal pressure	Usefulness-driven	Value-driven	Interest-driven
Type of ERSB	None	Organizational compliance	Sportsmanship	Civic virtue	Helping	Helping
			Individual initiative Civic virtue	Whistleblowing Individual initiative	Stewardship Civic virtue	Civic virtue Individual initiative
Motivators of ERSB	Laziness	Obedience	Praise / Recognition / Acknowledgment	High security awareness and sensitization	Desire to protect others	Personal interest
	Lack of time	ISP compliance	Encouragement	Understanding the importance of IT security	Altruistic values	Enjoyment in helping
	Lack of ideas	Salary increase	Managers lead by example	Sense of responsibility	Personal code of conduct	Enjoyment in being involved
	Lack of interest / apathy	Promotion	Social pressure	Perceived usefulness for private context	Personal concern / experience	Technophilia
	Lack of expertise / competence/ self-efficacy	Threats of sanction	Culture of constructive criticism	Desire to take the pressure of IT personal		
	Dominance of IT management		Organizational culture integrates IT security / unwritten norms	Overconfidence		
	Resistance to completion of tasks outside one's scope of duties		Self-protection	Self-protection		
	Responsibility shift		Loyalty to colleagues			

Motivators in the second extrinsic category are attributed to internal pressure in terms of following the expectations of others and wanting the approval of others (Gagné and Deci, 2005). Many interviewees report a higher motivation for ERSB when receiving **praise**, recognition or acknowledgment for it. In alignment with related research (e.g., Bénabou and Tirole 2003, Deci et al. 1999, Deci and Ryan 1985, Kohn 1993), one employee reports that *"praise and recognition motivate better than monetary compensation in the long run*" (P16). When the IT department or superiors specifically **encourage** employees' involvement in information security matters and support employees' initiative, employees are more likely to follow these expectations and perform ERSB. Such expectations also arise when IT security is integrated in the organizational culture and it becomes an **unwritten norm** to, for instance, openly communicate about security incidents. A **culture of constructive criticism** focuses on how a security problem at hand can be solved and prevented in the future rather than looking for someone to blame (*"Getting employees to do more than they have to requires a certain attitude, and we achieve this through training and by making them aware that they are part of a whole.", P29*). For instance, Frank (2020) shows that employees who work in a trusting and supportive environment have fewer concerns when it comes to sharing information security failures. Managers that **lead by example** and perform ERSB play to this internal pressure as well. It seems to be especially important that managers react with a high amount of sensitivity when someone shares their experience with a security incident or proposes improvement suggestions. Similarly, eager colleagues who perform ERSB can build a **peer pressure** to also engage in ERSB. Social pressure – i.e., influence in the form of normative beliefs and observed behavior of significant others – has been found to affect one's intentions to comply with security guidelines (Herath and Rao, 2009) and information security policies (Wang et al., 2022). On the other hand, **loyalty** to colleagues and concerns about betraying their trust may prevent an employee from reporting security issues involving others (*"I would not report my colleagues.", P26*). The existence of easy processes and **opportunities** to perform ERSB further increases employees' motivation to do so. For instance, if VPN can be turned on in just a click, more employees might choose to do so even when it is not mandatory to use it. Finally, **self-protection** is a strong motivator to perform ERSB. Drawing on protection motivation theory individuals are motivated to protect themselves when they are afraid of a certain outcome of an action (Rogers, 1975). To give an example: Employees are willing to participate in ERSB if they feel it will protect them from sanctions and criticism or save them from an embarrassing situation ("*I think it would be embarrassing [...] if I did something that was not good [...]*", P06). Most of the motivators in this category translate best to the ERSB types of sportsmanship, civic virtue, and individual initiative.

Three categories along the SDT draw on somewhat autonomous sources of motivation ("wantification"). The first one encompasses usefulness-driven motivation regulators. For instance, **understanding** the importance of IT security causes employees to perceive ERSB as relevant, valuable and useful. Repeated, vivid security trainings help raise **security awareness and sensitization** as well as a **sense of responsibility** in terms of having a mindset that each person is part of and contributes to the organization's IT security. Motivation for ERSB increases when it is considered useful for private context as well, for instance if the content of a voluntary training is **transferable** to an employee's home setting. Some employees feel the **desire to reduce the workload of IT personnel** by showing initiative and trying to solve IT security matters themselves (*"We try to help each other with IT security problems to reduce the workload on the IT department.", P09*). Typically, these employees are highly confident in their skills and knowledge. However, this Is a red flag as **overconfidence** can trigger harmful ERSB. We will discuss this double-edged sword effect of ERSB further in Chapter 5. The motivators identified in this category typically lead to the ERSB type of individual initiative and whistleblowing.

The next category is value-driven as motivators in this category fit with an employee's deeply held values. Nearly all employees state they would perform ERSB to protect others. Many mention the **desire to protect** their colleagues from abuse, critique, sanctions or a negative experience in general (e.g., *"When I see colleagues being sloppy, I talk to them to prevent them from being* *flagged.", P23*). This is especially the case for older employees or new members of the team. The desire to protect the organization and its reputation drives employees to perform ERSB. For instance, some feel their organization deserves a good security-behavior beyond simple compliance and many want to perform ERSB to protect the data of customers and stakeholders. Another motivator is personal concern for IT security due to prior **personal experience** with security incidents. Tatu et al. (2018), for instance, show that prior incident experience increase employees' information security awareness. And those who show higher levels of information security awareness are more willing to perform extra-role security behaviors, such as helping and whistleblowing (Jaeger and Eckhardt, 2018). Performing ERSB in these instances represents a synthesis with self. Having a **personal code of conduct** or certain personality traits such as being attentive or having a high general threat awareness seems to trigger ERSB. Overall, **altruistic values** greatly benefit ERSB, especially helping, stewardship, civic virtue and organizational loyalty.

Motivators in the last category are purely intrinsic and interest-driven. They encompass a personal **interest in IT security**, which manifests itself, for instance, in taking pleasure from learning about new trends in IT security through videos or articles in one's free time *("Well, [it] is part of the extra-occupational study program, and there are also modules that focus on IT security. Accordingly, I would say that I am also continuing my education in the personal realm as far as this topic is concerned.", P15)*. **Enjoying helping** others with security-related issues, **enjoying being involved** and having a strong enthusiasm for new technologies drive ERSB as well. Typically, these motivators trigger the following ERSB: helping, civic virtue, individual initiative and self-development.

4.2.2. Discussion and implications

SDT states that while external sources of motivation may be beneficial to achieve a goal (here: maximizing ERSB), it is more important for people to draw on internal sources of motivation. It claims that intrinsic motivation leads to a sense of gratitude, energy, deep learning and persistence, whereas extrinsic motivators trigger behavior to avoid feelings of shame, guilt, tension and anxiety (Ryan and Deci, 2000). To become self-determined, peoples' needs for autonomy, competence and connection need to be fulfilled (Ryan and Deci, 2000). Autonomy is present when employees perceive that they are able to take direct actions. In the IT security context, this can be encouraged by welcoming employees' suggestions on IT security matters and presenting appropriate channels to get involved. However, as established in the previous chapter, not all ERSBs are desirable and it can be harmful to encourage a feeling of autonomy regarding all IT security matters. Establishing boundaries of ERSB and encouraging autonomy within these constraints is a good compromise.

Competence – which is fulfilled when people have the necessary skills to enhance IT security – can be increased through trainings and creating an awareness on beneficial ERSB that is implementable without technical knowledge (e.g., using a privacy filter or reporting suspicious e-mails). Our interview data shows that often employees who are willing to engage in ERSB simply do not know how. Providing them with a sense of competence and concrete ideas on how to get involved will likely motivate them to perform ERSB. Measures such as team-building exercises and dedicated meetings that enhance a feeling of being connected to colleagues, managers and the organization further the internalization of security-related motivation, as they might increase the desire to protect others from security incidents. Positive relational ties also prevent workers from using neutralization techniques for their own illicit behavior or for colleagues' policy violations (Frank, 2021). Considering that employees with higher self-efficacy are more likely to fear negative consequences, Kwak et al. (2020) suggest improving communication between employees reporting phishing emails and the portals handling these reports to increase reporting rates.

Influencing intrinsic motivation proves more complicated than putting in place measures to increase extrinsic motivation (Bénabou and Tirole, 2003). There is no straightforward path to arising genuine interest and creating deeply held values in line with IT security. Acknowledging employees' feelings, giving them choices and opportunities for self-direction are shown to enhance intrinsic motivation by providing a feeling of autonomy (Deci and Ryan, 1985). Influencing somewhat internal, usefulness-driven motivations seems promising as well. Security education training and awareness (SETA) programs have a proven potential to increase employees' security awareness and sensitization and establish a collective mindset of responsibility for IT security at a relatively low-cost (Straub and Welke, 1998; Whitman, 2003). If employees feel responsible for change (Nehme and Marler, 2023) and identify with their role as information security end-users (Ogbanufe and Ge, 2023), they are more willing to engage in extra-role security behaviors.

Providing platforms and opportunities such as regular meetings for employees to share experiences with IT security-related incidents could spread personal concern for the topic among colleagues and build an understanding of the importance of IT security. Previous research has already shown that sharing experiences positively influences security awareness (Tatu et al., 2018). At the same time, employees who are generally more aware of security threats and policies tend to participate more in sharing experiences (Frank and Ament, 2021). Creating a culture of constructive criticism and open communication, training managers to lead by example, acknowledging ERSB and establishing opportunities and easy processes for ERSB are promising approaches to enhancing an internal pressure to engage in ERSB. One promising avenue to pursue is humble leadership, as it can create a positive work climate that encourages employees to talk about personal experiences with information security incidents (Frank, 2020). It also seems advisable to emphasize the role of employees as the first line of defense, for example, by helping them develop strong password strategies or giving them space to learn from security incidents without pointing the finger at individuals (Zimmermann and Renaud, 2019). Organizations need to be aware that focusing on enhancing extrinsic motivation (e.g., through punishments and rewards) undermines intrinsic motivation, as previous literature has shown that, for instance, financial incentives dampen altruism (Frank and Ament, 2021; Qiao et al., 2020) or that pressure to perform ERSB can lead to security violations (Jia and Xu, 2021). In general, it seems advisable for companies to find out which employees are driven by which motivational factors. This could help better tailor interventions to employees and encourage behaviors that go beyond what is prescribed in security policies. Machine learning is one of the methods that has already been successfully used recently to study behavior-based information security (Frank et al., 2023).

In summary, we have identified various motivators of ERSB for each type. Table 4 provides a brief summary of the results and their practical implications. We can conclude that introducing measures to strengthen the identified motivators or to minimize sources of amotivation has the potential to increase employees' ERSB. When designing and implementing such measures, we advice organizations to differentiate between groups of employees. We recommend an initial screening to identify employees with a high intrinsic motivation as demonstrated through a high self-reported interest in IT security and the desire to learn more about it and be more involved. For this group it is especially important to raise awareness of what boundaries should be respected with regard to ERSB.

Table 4
Practical implications.

General Findings	Practical Implications
Extra-role security behaviors are a double-edged sword	• Setting boundaries according to corporate strategy and balancing employees' need for autonomy with information security regulation
Competence fosters extra-role behavior	• Empower employees to act safely by training and raising awareness of prosocial behaviors that can be implemented without technical knowledge
Employees exhibit different types of extra-role behaviors that are based on different motivating factors	• Identify employees who fall into these categories in order to better steer and foster extra-role behaviors
Autonomy fosters extra-role security behaviors	• Empower employees to take action, for example, by providing platforms for them to engage and share experiences
Sense of connection promotes extra-role security behaviors	• Establish positive working relationships, e.g., by strengthening goals and individual roles in combatting security attacks and mitigating risks
A culture of constructive criticism promotes extra-role security behaviors	• Create a work environment where employees feel safe and can talk openly about security incidents, experiences, and failures

While this may look different in each organization, a good starting point is to clarify that ERSBs should never conflict with ISPs and that the help desk should be consulted before questionable actions are taken. Help desks are commonly viewed as a valuable source of expertise, security guidance and updating employees' security knowledge (Al Awawdeh and Tubaishat, 2014). For those employees showing neither interest in IT security nor IT know-how, the demonstration of simple examples of ERSB that can be implemented with little effort and knowledge might increase their self-confidence regarding their ability to contribute to IT security. This goes hand in hand with building a common understanding that IT security involves everyone and despite of errors the human factor is able to play a positive role in securing organizational assets (Zimmermann and Renaud, 2019).

As both extrinsic and intrinsic motivators might trigger potentially harmful ERSB, organizations need to be aware that introducing incentives for ERSB is accompanied by this risk. Conducting a careful risk assessment helps establish which kinds of ERSBs should be encouraged and which risks can be tolerated in the process.

5. Double-edged sword effect of extra-role security behavior

5.1. Initial findings

Previous research on extra-role security behaviors looks largely to Hsu et al. (2015) who conceptualize extra-role security behavior as facilitating organizational functioning and, in particular, increasing compliance with information security policies. Indeed, research that followed examined different aspects of extra-role security behaviors, such as antecedents or consequences (e.g., Jaeger and Eckhardt 2018), but still focused almost exclusively on the positive sides of ERSB while overlooking potentially adverse consequences of such behaviors. To the best of our knowledge, only Jia and Xu (2021) examine under which condition extra-role security behavior might lead to negative outcomes. Based on the 29 interviews we analyzed, it appears that some extra-role security-behaviors, even if well-intentioned, can have negative effects, such as affecting compliance with information security policies. Take helping as one of the extra-role security behaviors, for instance: Employees perceive they have sufficient security knowledge to follow the companies' security regulations. They even volunteer to share their knowledge with colleagues who ask them for advice on security questions. However, even if they mean well, the knowledge they pass on may not be accurate and their advice may be of low quality. As a result, their prosocial behavior may do more harm than good, i.e., torpedoing compliance with security policies. Some of our respondents therefore believe that asking non-IT staff to help with troubleshooting is not a good idea. A 28-year-old team leader in human resources controlling said, "*security issues are too important to try to help others with half-knowledge."*

Security issues also appear to arise in another ERSB category, namely individual initiative. Respondents mentioned that they had chosen to implement security measures that were not explicitly approved by their employer. For instance, one interviewee reported that he decided to remove one of the security updates because he thought it was flawed. This clearly violates the company's security policies and puts him at risk of falling victim to cybercriminals. It appears that several dimensions of ERSB have an ambivalent influence on the effectiveness of information security compliance. Consequently, we can establish that ERSBs contribute unevenly to the effectiveness of information security policy compliance. In the following, and based on our interview findings, we seek to explain how this ambivalent influence relates to ISP compliance, what might contribute to the development of harmful ERSB and what determines who perceives ERSB as ambiguous.

5.2. Psychological distance and extra-role security behavior

It is incontestable that leaders play a significant role in information security, for instance with regard to motivating prosocial behaviors as a means to increase protection against security threats (Guhr et al., 2019; Posey et al., 2013). However, according to our results, they seem to have a differentiated opinion on whether prosocial behaviors are disruptive or not. While some leaders are strictly against the performance of ERSB, such as helping or being proactive, others are more open to ERSB and welcome it. For instance, a 50-year-old female leader who works in finance reported that the company's IT director does not want them to help each other but wants to maintain control over what is communicated and done regarding information security. Another respondent who works in human resources controlling and has managerial responsibilities explained her reluctance to support ERBS as follows: "*Security questions are too important to try to solve with superficial knowledge or do it off the top of one's head*". This is consistent with other managers who indicated that they do not encourage their workforce to helping each other because they may pass on erroneous information. In contrast, one team leader who works in development reported that sharing information security experiences is helpful in raising awareness.

In order to understand why leaders differ in their evaluation of extra-role security behaviors, we draw on the psychological distance of construal level theory (CLT). CLT assumes that humans think in concrete ways about objects and events close to them, whereas they think in abstract ways about objects and events perceived as distant (e.g., memories, plans, predictions, hopes, counterfactual alternatives) (Eyal et al., 2008; Liberman et al., 2007; Trope and Liberman, 2010). Psychological distance can occur in four dimensions: Temporal distance (whether an event happens now or in the distant future), spatial distance (whether or not it occurs in close physical proximity), social distance (whether it is happening to oneself or similar others) and hypothetical distance (whether or not the occurrence of an event is likely) (Trope and Liberman, 2010). People associate one type of distance from an immediate experience with the others, as they automatically perceive anything far in one way as far in all other ways as well (Maglio et al., 2013).

While CLT often frames research on consumer behavioral decision-making (Fiedler, 2007), it is scarcely applied in IS security research. Orazi et al. (2019) created a construal level taxonomy for the design of fear appeals, in which they identified potential confounds in fear appeal manipulations. Kaleta et al. (2019) found that people thinking at a higher construal level choose stronger online passwords. Jaeger et al. (2017) proposed that information security awareness increases when temporal, spatial, social or hypothetical distance to information security incidents decreases. They further found that psychological distance is reduced when a security champion – a self-declared mediator of information security – is present in the team. However, to the best of our knowledge, we are the first to apply CLT and psychological distance to ERSB.

Since the occurrence or nature of security incidents is not foreseeable, employees typically perceive them as being in an unknown distant future (temporal distance) or assume they will happen somewhere else (spatial distance), to others (social distance) or not at all (hypothetical distance). Thus, mental representations of information security incidents are construed on a high level, resulting in more abstract (vs. concrete) thoughts (Trope and Liberman, 2010; Wakslak et al., 2006). ERSB performed under these conditions does not focus on a specific security incident but encompasses preventive measures (e.g., changing passwords more frequently than required) and educational measures (e.g., participating in voluntary trainings). These high-level actions have little to no potential to do any harm and should be encouraged by organizations.

As indicated by prior research, psychological distance impacts employees' information security awareness (Jaeger et al., 2017). Being more aware of information security means that employees are more aware of the potential consequences that come along with security incidents. One of the IT managers explained that as an IT employee they need to take a leading role in ensuring that users understand and are aware of policies and report security incidents to the right people. Most leaders also acknowledge that information security incidents happen more frequently, meaning they show low temporal distance. Leaders working in IT even have expert knowledge on the subject because their job role entails gaining information about IT security-related events or objects firsthand. Consequently, they promote information security awareness and strive for an understanding that every employee contributes to IT security. However, because of their low experiential distance, they see several ERSB dimensions as challenging for information security and prefer to have employees report critical behaviors rather than have them help one another.

5.3. Overconfidence and extra-role security behavior

Feeling overly confident might cause misjudgments of one's actual security competence, skills and knowledge (Howah and Chugh, 2019). Previous studies confirm the risks associated with overconfidence in IT security (Aggarwal et al., 2015; Frank, 2020; Hewitt and White, 2020; Howah and Chugh, 2019; Schmidt et al., 2007; Wang et al., 2016). A common motive for amotivation concerning ERSB found in our interviews is feeling too insecure to perform security-related activities voluntarily. Most often, this insecurity was reported by employees working in non-IT departments. For instance, a marketing and sales advisor (P05) stated: *"I just don't think I am helpful, and I think I am too scared to say something wrong."* While these concerns prevent beneficial ERSB, they also protect from potentially harmful ERSB. In fact, all examples of potentially dangerous ERSB observed in our study were reported by employees with an IT background who justified their actions with deep subject knowledge and years of experience. For instance, a business analyst in IT (P18) reported: "*I have voluntarily rolled back a system update several times when I realized that it would not meet the security requirements. Since I come from the field, I have enough know-how to do this.*" While this action does not necessarily lead to an increased security risk for the future or might in fact decrease said risks, the fact alone that they felt confident enough to circumvent the official rules is a potential risk. In another example, a manager in an IT consultancy (P22) testified: "*I have voluntarily installed a virus scanner at my own expense on the cell phone that I use for private and business purposes, because I do many important things with it and open sensitive data and because I am sensitized due to my many years of experience.*" Installing external software on a device used for business purposes without clearance from the IT security department is a potential risk. Companies often employ configuration management, which controls what software is installed on which devices, to restrict the windows through which malware might enter. Installing third-party software – even if it is a virus scanner – defeats that purpose.

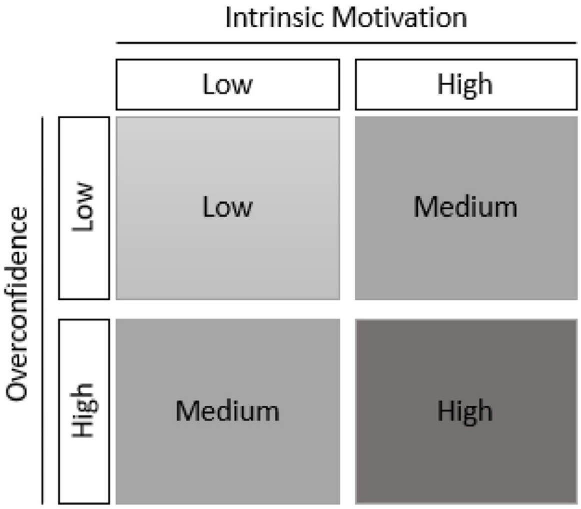

Fig. 3. Risk assessment framework for extra-role security behavior.

5.4. Risk assessment framework

Previous literature demonstrates the benefits ERSB can have for an organization's information security (Hsu et al., 2015; Jaeger and Eckhardt, 2018). So far, little attention has been paid to the risks that are inevitably introduced along with the emergence of ERSB. Through the application of self-determination theory, we demonstrated the superior role intrinsic motivation plays in both harmless as well as potentially harmful ERSB across all types (see Chapter 4.2). In the previous chapter (5.3), we proposed overconfidence as a risk factor for harmful ERSB. Based on these combined findings, we developed the following framework to assess the level of risk associated with ERSB (see Fig. 3). It is, to the best of our knowledge, the first attempt to provide support in managing the double-edged sword effect of ERSB.

As shown in Fig. 3, employees with low self-confidence and little intrinsic motivation are at the lowest risk of performing harmful ERSBs. Employees with high overconfidence but low intrinsic motivation or employees with low overconfidence and high intrinsic motivation are at medium risk. And employees who show both high intrinsic motivation and high overconfidence represent the highest risk category.

Because employees with high levels of overconfidence and intrinsic motivation are more likely to engage in harmful ERSB, it is advisable for employers to assess 1) their employees' level of intrinsic motivation and 2) their levels of overconfidence with respect to information security. This can be done, for example, by asking questions about personal interest in information security, security-related values, personal experiences with security incidents, desire to get involved, etc. Assessing overconfidence in information security can be done using security questionnaires such as those used by Ament (2017) and Frank et al. (2023). In additions, efforts are needed in this quadrant to clarify and emphasize the boundaries of ERSB (e.g., adhering to ISPs for every security-related action and regularly reminding employees to seek second opinions on critical security matters).

Employees with low intrinsic motivation rarely perform ERSB. To profit from the benefits of ERSB, it is advisable to encourage these employees to engage in ERSB, for instance, by showing them examples of uncomplicated and easy ERSB and boosting their confidence that they capable of performing similar actions despite little technical know-how. However, it is important to prevent them from becoming overconfident, as this promotes harmful ERSB. It should be noted that this matrix, derived from the interview results, is an initial attempt to assess risks related to prosocial security behaviors. Consequently, there may be other risk factors that promote harmful ERSB and that complement the proposed matrix for a more granular assessment of ERSB risks. To identify these, it is necessary to study historical data and collaborate with security experts.

6. Limitations and future work

Although our findings are encouraging and contribute to a deeper understanding of extra-role security behaviors, we acknowledge certain limitations. These limitations, however, also open new avenues for future research. First, qualitative research studies are often criticized for lacking credibility and validity (Creswell and Miller, 2000). We, therefore, relied on triangulation across participants and investigators to go through our data (interviews) to find common categories of extra-role security behaviors. This seems to be an appropriate approach, as information systems research lacks a general understanding of what types of extra-role security behaviors exist and what motivates them.

Like most studies of extra-role security behavior, this qualitative research is based on insights from a variety of Western organizations. While we argue that this helps us to unfold extra-role security behaviors in the best interpretivist manner, it also opens up opportunities for comparative studies (Lee and Baskerville, 2003). Research from other disciplines show extra-role behaviors and its motivations may differ in different cultural settings (Wollan et al., 2009). And preliminary findings in the field of information security suggest that in China peer pressure has a positive effect on extra-role security behaviors (Wang et al., 2022), whereas in Western societies social pressure is thought to negatively affect prosocial behaviors and lead to security violations (Jia and Xu, 2021). With this in mind, it is to be expected that extra-role security behavior is also influenced by the cultural background of the individuals studied, which makes further research worthwhile.

Although researchers generally agree that extra-role security behaviors are spontaneous and should not be constrained by punishment and reward there is disagreement about what types of extra-role security behavior exists. Therefore, the goal of our work was to shed some light on which categories of extra-role security behavior exists and why. Our results suggest that being compliant without anyone seeing should be considered extra-role security behavior. This contrasts with scholars who classify organizational compliance as in-role behavior (Chen and Li, 2019). It seems that the boundary between in-role and extra-role behavior sometimes remains indistinct.

Given the importance of extra-role security behavior in enhancing information security policy effectiveness (Hsu et al., 2015), our works contributes to the growing body of literature in this area while being one of the first to examine not only the positive but also the negative effects of these types of security behaviors. We therefore hope that our study will encourage other researchers to also explore the detrimental side of extra-role security behaviors. The framework presented provides a solid first foundation for future studies by contributing to the understanding of motivational factors that impact the performance of extra-role security behavior. Researchers, for instance, can use the framework to develop a measurement model and provide quantitative evidence of our findings. Another promising avenue for future research may be the exploration of extra-role behaviors using longitudinal studies, as they allow researchers to collect actual data that cannot be captured in snapshot surveys (Kim and Malhotra, 2005; Venkatesh and Davis, 2000).

Besides, the discovery of the double-edged sword effect of extra-role security behaviors underscores the importance of security awareness training. Guan and Hsu (2022) advocate for information security mindfulness to encourage employees to engage in extra-role security behavior. Thus, as a next step, it would be interesting to investigate whether mindfulness can help to reduce the potential negative outcomes of certain extra-role security behaviors. Based on our findings, setting boundaries for extra-role security behaviors while encouraging autonomy within these boundaries seems to be a good starting point for further research. Jia and Xu (2021), for instance, advice managers not to push employees to engage in extra-role security behaviors. Therefore, scholars should explore how to best encourage employees to act prosocial while preventing security deviations.

7. Conclusion

This exploratory study examined different types of extra-role security behaviors and challenged the positive view that research previously held about these types of behaviors.

We identified and analyzed nine types of ERSB with regards to their manifestation in an organizational context, associated challenges, and underlying motivators. Our findings suggest that extra-role security behaviors contribute to varying degrees to the effectiveness of information security compliance. For instance, ERSB of the type helping is typically either usefulness-driven, value-driven or interest-driven and includes behaviors such as sharing security-related knowledge or helping colleagues with security-related problems. However, the benefit of helping goes hand in hand with the risk of a potential spread of incorrect advice that could harm the organization. We are - to the best of our knowledge - among the first to take a differentiated look at the unwanted side effects of positively intended extra-role security actions. We refer to this phenomenon as the double-edged sword effect of ERSB. Organizations need to be aware that attempting to increase ERSB of any kind - for example, by creating a culture of constructive criticism and open communication - also introduces security-related risks. Drawing on the level of intrinsic motivation and overconfidence, we derived initial indication for conducting a risk-benefit assessment. All in all, this work provides a more holistic understanding of extrinsic and intrinsic motivation with respect to prosocial security behaviors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

This research was funded in part by PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Appendix A
Interview protocol.

Block: Demographic data		
Main Question	Detail Question	Reason and Objective
- How old are you?		Demographic Data
- What is your gender?		Demographic Data
- What is your highest level of education (e.g., Bachelor, Master, vocational training)?		Demographic Data
- How many years of work experience do you have?		Demographic Data
- What is your job position (e.g., Business Analyst, IT Consultant, etc.)?		Demographic Data
Block: General Attitude Towards IT Security and Security Awareness		
- Does your company have mandatory IT security policies?	Which for example?	Insights about companies' information security strategy
- What does IT security mean to you in your workplace?		Opinion on information security in the workplace
- How important or unimportant is IT security in the workplace to you? 1 - not at all important 2 - unimportant 3 - neutral 4 - important 5 - very important		Attitude towards information security in the workplace
- And in comparison, what does IT security mean to you in your private life?	How does it affect your work?	Attitude towards information security at home
- How do you see your role in terms of IT security?		Understanding one's role in information security
- Does your company have mandatory IT security policies? - What does IT security mean to you in your workplace? - How important or unimportant is IT security in the workplace to you? 1 - not at all important 2 - unimportant 3 - neutral 4 - important 5 - very important		IT security awareness
- What security awareness activities are you aware of and have you participated in any?		IT security awareness
Block: Extra-role Security Behaviors		
- Have you ever engaged in behaviors that go beyond your information security obligations?	Which? And why?	Insights on people's extra-role security behaviors
- Are you encouraged to share your experiences, both positive and negative, regarding IT security?	If so, how?	Insights on people's extra-role security behaviors
- Are people in your department encouraged to get involved in security issues, i.e., to make suggestions for improvement, and to help each other with IT security problems?	If so, how?	Insights on people's extra-role security behaviors
- Have you ever witnessed a colleague circumventing IT regulations?	If so, what did you do about it?	Insights on people's extra-role security behaviors
- What circumstances would you have to face in order to take (more) voluntary measures that serve IT security in your company?		Motivation for extra-role security behaviors
- Which of the following would encourage you to engage in voluntary actions and non-mandated behaviors that promote IT security in your organization? - Recognition from superiors or colleagues (reputation) - Monetary compensation - Measures in the company that increase my IT security awareness and knowledge. - Being more responsible in front of superiors and colleagues because of such measures. - Have you ever witnessed a colleague circumventing IT regulations? - What circumstances would you have to face in order to take (more) voluntary measures that serve IT security in your company? - Which of the following would encourage you to engage in voluntary actions and non-mandated behaviors that promote IT security in your organization? - Recognition from superiors or colleagues (reputation) - Monetary compensation - Measures in the company that increase my IT security awareness and knowledge. - Being more responsible in front of superiors and colleagues because of such measures.		Motivation for extra-role security behaviors

(*continued on next page*)

Appendix A (*continued*)

Block: Demographic data Main Question	Detail Question	Reason and Objective
Block: Security Incidents and Error Culture		
- Have you ever had a security incident happen at work or have you ever identified a security risk? If so, what did it look like (roughly)?	How did you deal with the incident? If you have not done anything: Why didn't you do anything? Otherwise: Why did you implement the measures you mentioned? Which of these following statements are true or not true when you consider what influenced your decision to take these actions? a. I care about what happens to the company. b. I want to prevent others from having a similar negative experience. I want to protect the company. c. I think it would benefit my reputation. d. I feel committed to the company. e. I want to help my colleagues where I can. f. I like to exchange ideas with others, in the sense of sharing experience, for example. Other reasons:	Incident experience and motivators for (not) taking actions
Optional Block: Case Studies		
Case 1: Imagine that your colleague walks away from the workplace without locking his/her screen. What would you do and why?		Exploring people's extra-role security behaviors
Case 2: Imagine you received an e-mail from your customer making a request that violates IT security policies (e.g., sending certain documents to his/her private e-mail because he/she doesn't have access to his/her work laptop). What would you do and why?		Exploring people's extra-role security behaviors

References

Aggarwal, R., Kryscynski, D., Midha, V., Singh, H., 2015. Early to adopt and early to discontinue: the impact of self-perceived and actual IT-knowledge on technology use behaviors of end users. Inf. Syst. Res. 26 (1), 127–144.

Ament, C., 2017. The ubiquitous security expert: overconfidence in information security. In: Proceedings of the 38th International Conference of Information on Information Systems, pp. 1–18.

Ament, C., Haag, S., 2016. How information security requirements stress employees. In: Proceedings of the 37th International Conference on Information Systems (ICIS), pp. 1–17.

Al Awawdeh, S., Tubaishat, A, 2014. An information security awareness program to address common security concerns in IT unit. In: Proceedings of the International Conference on Information Technology: New Generations, pp. 273–278.

Barriball, K.L., While, A., 1994. Collecting data using a semi-structured interview: a discussion paper. J. Adv. Nurs. 19 (2), 328–335.

Bénabou, R., Tirole, J., 2003. Intrinsic and extrinsic motivation. Rev. Econ. Stud. 70 (3), 489–520.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34, 523–548.

Castilla, E.J., Ranganathan, A., 2020. The production of merit: how managers understand and apply merit in the workplace. Organ. Sci. 31 (4), 909–935.

Chen, B., Vansteenkiste, M., Beyers, W., Boone, L., Deci, E.L., Van der Kaap-Deeder, J., Duriez, B., et al., 2015. Basic psychological need satisfaction, need frustration, and need strength across four cultures. Motiv. Emot. 39 (2), 216–236.

Chen, H., Li, W., 2019. Understanding commitment and apathy in IS security extra-role behavior from a person-organization fit perspective. Behav. Inf. Technol. 38 (5), 454–468.

Cram, W.A., D'Arcy, J., Proudfoot, J.G., 2019. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Q. 43 (2), 525–554.

Cram, W.A., Proudfoot, J.G., D'Arcy, J., 2017. Organizational information security policies: a review and research framework. Eur. J. Inf. Syst. 26 (6), 605–641 Palgrave Macmillan UK,.

Creswell, J.W., Miller, D.L., 2000. Determining validity in qualitative inquiry. Theory Pract. 39 (3), 124–130.

D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. J. Manag. Inf. Syst. 31 (2), 285–318.

D'Arcy, J., Hovav, A., Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. 20 (1), 79–98.

D'Arcy, J., Lowry, P.B., 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study. Inf. Syst. J. 29 (1), 43–69.

Deci, E.L., 1971. Effects of externally mediated rewards on intrinsic motivation. J. Personal. Soc. Psychol. 18 (1), 105–115.

Deci, E.L., Koestner, R., Ryan, R.M., 1999. A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. Psychol. Bull. 125 (6), 627–668.

Deci, E.L., Ryan, R.M., 1985. Intrinsic Motivation and Self-Determination in Human Behavior. Springer Science & Business Media, Berlin.

Deci, E.L., Ryan, R.M., 1987. The support of autonomy and the control of behavior. J. Personal. Soc. Psychol. 53 (6), 1024–1037.

Van Dyne, L., Cummings, L.L., McLean Parks, J., 1995. Extra-role behaviors: in pursuit of construct and definitional clarity (a bridge over muddied waters)". Res. Organ. Behav. 17, 215–285.

Van Dyne, L., Graham, J.W., Dienesch, R.M., 1994. Organizational citizenship behavior: construct redefinition, measurement, and validation. Acad. Manag. J. 37 (4), 765–802.

Van Dyne, L., LePine, J.A., 1998. Helping and voice extra-role behaviors: evidence of construct and predictive validity. Acad. Manag. J. 41 (1), 108–119.

Eyal, T., Liberman, N., Trope, Y., 2008. Judging near and distant virtue and vice. J. Exp. Soc. Psychol. 44, 1204–1209.

Fiedler, K., 2007. Construal level theory as an integrative framework for behavioral decision-making research and consumer psychology. J. Consum. Psychol. 17 (2), 101–106.

Frank, M., 2020. Sharing information security failure: the role of social context and social environment. In: Proceedings of the 23rd Pacific Asia Conference on Information Systems, pp. 1–14.

Frank, M., 2021. Combatting the neutralization of security policy violations: insights from the healthcare sector. In: Proceedings of the ECIS. available at.

Frank, M., Ament, C., 2021. How motivation shapes the sharing of information security incident experience. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 4528–4537.

Frank, M., Jaeger, L., Ranft, L.M., 2023. Using contextual factors to predict information security overconfidence: a machine learning approach". Comput. Secur. 125, 103046 Elsevier Ltd.

Frank, M., Ranft, L.M., 2021. Using machine learning to explore extra-role security behavior. In: Proceedings of the 42nd International Conference on Information Systems, pp. 1–17.

Gagné, M., Deci, E.L., 2005. Self-determination theory and work motivation. J. Organ. Behav. 26 (4), 331–362.

George, J.M., Brief, A.P., 1992. Feeling good-doing good: a conceptual analysis of the mood at work-organizational spontaneity relationship. Psychol. Bull. 112 (2), 310–329.

Guan, B., Hsu, C., 2022. Investigating employees' proactive extra-role information security behaviors through security mindfulness. In: Proceedings of the ICIS, pp. 0–9.

Guhr, N., Lebek, B., Breitner, M.H., 2019. The impact of leadership on employees' intended information security behaviour: an examination of the full-range leadership theory. Inf. Syst. J. 29 (2), 340–362.

Guo, K.H., 2013. Security-related behavior in using information systems in the workplace: a review and synthesis. Comput. Secur. 32 (1), 242–251 Elsevier Ltd.

Harry, B., Sturges, K.M., Klingner, J.K., 2015. Mapping the process: an exemplar of process and challenge in grounded theory analysis. Educ. Res. 34 (2), 3–13.

Herath, T., Rao, H.R., 2009. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47 (2), 154–165 Elsevier B.V..

Hewitt, B., White, G.L., 2020. Optimistic bias and exposure affect security incidents on home computer. J. Comput. Inf. Syst. 1–11 Taylor & Francis.

Howah, K., Chugh, R., 2019. Do we trust the internet? Ignorance and overconfidence in downloading and installing potentially spyware-infected software. J. Glob. Inf. Manag. 27 (3), 87–100.

Hsu, J.S.C., Shih, S.P., Hung, Y.W., Lowry, P.B., 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. Inf. Syst. Res. 26 (2), 282–300.

Hu, S., Hsu, C., Zhou, Z., 2021. The impact of SETA event attributes on employees' security-related Intentions: an event system theory perspective. Comput. Secur. 109, 102404.

Jaeger, L., Ament, C., Eckhardt, A., 2017. The closer you get the more aware you become – a case study about psychological distance to information security incidents. In: Proceedings of the ICIS, pp. 0–18.

Jaeger, L., Eckhardt, A., 2018. When colleagues fail: examining the role of information security awareness on extra-role security behaviors. In: Proceedings of the 26th European Conference on Information Systems (ECIS), 2018 2015.

Jia, S., Xu, F., 2021. When extra-role behavior leads to employee security deviance: a moral licensing view. In: Proceedings of the Annual Americas Conference on Information Systems, AMCIS, pp. 0–5.

Kaleta, J.P., Lee, J.S., Yoo, S., 2019. Nudging with construal level theory to improve online password use and intended password choice: a security-usability tradeoff perspective. Inf. Technol. People 32 (4), 993–1020.

Katz, D., 1964. The motivational basis of organizational behavior. Behav. Sci. 9 (2), 131–146.

Kelle, U., 1995. Computer-Aided Qualitative Data Analysis: Theory, Methods and Practice. Sage Publications, London.

Kim, B., Lee, D.Y., Kim, B., 2020. Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. Behav. Inf. Technol. 39 (11), 1156–1175 Taylor & Francis.

Kim, S.S., Malhotra, N.K., 2005. A longitudinal model of continued IS use: an integrative view of four mechanisms underlying postadoption phenomena. Manag. Sci. 51 (5), 741–755.

Klein, H.K., Myers, M.D., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Q. 23 (1), 67–94.

Kohn, A., 1993. Punished by Rewards: The Trouble with Gold Stars, Incentive Plans, A's, Praise and Other Bribes. Houghton Mifflin Company, Boston.

Kwak, Y., Lee, S., Damiano, A., Vishwanath, A., 2020. Why do users not report spear phishing emails? Telemat. Inform. 48, 101343 January.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H., 2014. Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. 37 (4), 1049–1092.

Lee, A.S., Baskerville, R.L., 2003. Generalizing generalizability in information systems research. Inf. Syst. Res. 14 (3), 221–243.

LePine, J.A., Erez, A., Johnson, D.E., 2002. The nature and dimensionality of organizational citizenship behavior: a critical review and meta-analysis. J. Appl. Psychol. 87 (1), 52–65.

Li, Y., Fuller, B., Stafford, T., Ellis, S., 2017. Beyond compliance: empowering employees' extra-role security behaviors in dynamic environments. In: Proceedings of the 23rd Americas Conference on Information Systems, pp. 1–5.

Li, Y., Stafford, T., Ellis, S., Fuller, B., 2021. Beyond extra-role security behaviors in large corporate settings: the case of 'tribal security. SSRN Electron. J. doi:10.2139/ssrn.3870574, available at.

Liberman, N., Trope, Y., Stephan, E., 2007. Psychological distance. In: Kruglanski, A.W., Higgins, E.T. (Eds.), Social Psychology. The Guilford Press, New York, pp. 353–381.

Maglio, S.J., Trope, Y., Liberman, N., 2013. The common currency of psychological distance. Curr. Dir. Psychol. Sci. 22 (4), 278–282.

Moorman, R.H., 1993. The influence of cognitive and affective based job satisfaction measures on the relationship between satisfaction and organizational citizenship behavior. Hum. Relat. 46 (6), 759–776.

Moorman, R.H., Blakely, G.L., 1995. Individualism-collectivism as an individual difference predictor of organizational citizenship behavior. J. Organ. Behav. 16, 127–142.

Morrison, E.W., 1994. Role definitions and organizational citizenship behavior: the importance of the employee's perspective. Acad. Manag. J. 37 (6), 1543–1567.

Nehme, A., Marler, L.E., 2023. Buying in and feeling responsible: a model of extra-role security behavior. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 4131–4138.

Newman, A., Miao, Q., Hofman, P.S., Zhu, C.J., 2016. The impact of socially responsible human resource management on employees' organizational citizenship behaviour: the mediating role of organizational identification. Int. J. Hum. Resour. Manag. 27 (4), 440–455.

Niemiec, C.P., Ryan, R.M., 2009. Autonomy, competence, and relatedness in the classroom: applying self-determination theory to educational practice. Theory Res. Educ. 7 (2), 133–144.

Ogbanufe, O., Ge, L., 2023. A comparative evaluation of behavioral security motives: protection, intrinsic, and identity motivations. Comput. Secur. 128, 103136 Elsevier Ltd.

Orazi, D.C., Johnston, A.C., Warkentin, M., 2019. Integrating construal-level theory in designing fear appeals in IS security research. Commun. Assoc. Inf. Syst. 45 (1), 397–410.

Organ, D.W., 1997. Organizational citizenship behavior: it's construct clean-up time. Hum. Perform. 10 (2), 85–97.

Padayachee, K., 2012. Taxonomy of compliant information security behavior. Comput. Secur. 31 (5), 673–680.

Pham, H.C., Pham, D.D., Brennan, L., Richardson, J., 2017. Information security and people: a conundrum for compliance. Australas. J. Inf. Syst. 21, 1–16.

Podsakoff, P.M., MacKenzie, S.B., 1994. Organizational citizenship behaviors and sales unit effectiveness. J. Mark. Res. 31 (3), 351–363.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879–903.

Podsakoff, P.M., Mackenzie, S.B., Paine, J.B., Bachrach, D.G., 2000. Organizational citizenship behaviors: a critical review of the theoretical and future research. J. Manag. 26 (3), 513–563.

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., Courtney, J.F., 2013. Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Q. 37 (4), 1189–1210.

Qiao, D., Lee, S.Y., Whinston, A.B., Wei, Q., 2020. Financial incentives dampen altruism in online prosocial contributions: a study of online reviews. Inf. Syst. Res. 31 (4), 1361–1375.

Rioux, S.M., Penner, L.A., 2001. The causes of organizational citizenship behavior: a motivational analysis. J. Appl. Psychol. 86 (6), 1306–1314.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114.

Ryan, R.M., Deci, E.L., 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. Am. Psychol. 55 (1), 68–78.

Saldaña, J., 2013. The Coding Manual for Qualitative Researchers. SAGE Publications, London available at doi:10.1108/qrom-08-2016-1408.

Schmidt, G., Tanner, M., Hayes, T., 2007. Computer security threats: student confidence in their knowledge of common threats. J. Bus. Leadersh. 3 No (1), 211–215.

Smith, C.A., Organ, D.W., Near, J.P., 1983. Organizational citizenship behavior: its nature and antecedents. J. Appl. Psychol. 68 (4), 653–663.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22 (1), 42–75.

Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Q. 22 (4), 441–469.

Tatu, T., Ament, C., Jaeger, L., 2018. Lessons learned from an information security incident: a practical recommendation to involve employees in information security. In: Proceedings of the 49th Hawaii International Conference on System Sciences, pp. 3736–3745.

Trope, Y., Liberman, N., 2010. Construal-level theory of psychological distance Yaacov. Psychol. Rev. 117 (2), 440–463.

Vallerand, R.J., 1997. Toward a hierarchical model of intrinsic and extrinsic motivation. Adv. Exp. Soc. Psychol. 29, 271–360.

Venkatesh, V., Davis, F.D., 2000. Theoretical extension of the technology acceptance model: four longitudinal field studies. Manag. Sci. 46 (2), 186–204.

Vey, M.A., Campbell, J.P., 2004. In-role or extra-role organizational citizenship behavior: which are we measuring? Hum. Perform. 17 (1), 119–135.

Visser, C. (2017), "The motivation continuum: self-determination theory in one picture", available at: http://www.progressfocused.com/2017/12/the-motivation-continuum-self.html.

Wakslak, C.J., Trope, Y., Liberman, N., Alony, R., 2006. Seeing the forest when entry is unlikely: probability and the mental representation of events. J. Exp. Psychol. Gen. 135 (4), 641–653.

Walsham, G., 2006. Doing interpretive research. Eur. J. Inf. Syst. 15 (3), 320–330.

Wang, C., Liu, C., Yao, J., Li, L., 2022. Research on influencing factors of extra-role information security policy compliance behaviour based on structural equation model. In: Proceedings of the 2nd International Conference on Education, Information Management and Service Science (EIMSS). Atlantis Press International BV, pp. 547–556.

Wang, J., Li, Y., Rao, H.R., 2016. Overconfidence in phishing email detection. J. Assoc. Inf. Syst. 17 (11), 759–783.

Whitman, M.E., 2003. Enemy at the gate: threats to information security. Commun. ACM 46 (8), 91–95.

Wollan, M.L., Sully de Luque, M.F., Grünhagen, M., 2009. Motives for helping: exploring cultural influences on extra-role behavior. Multinatl. Bus. Rev. 17 (1), 99–119.

Zimmermann, V., Renaud, K., 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int. J. Hum. Comput. Stud. 131, 169–187 Elsevier LtdJanuary.

Muriel Frank is a research associate at the University of Luxembourg in Luxembourg. She received her PhD in Information Systems from Goethe University Frankfurt, Germany. Her research on behavioral information security and sociotechnical systems realignment has been published in several conference proceedings and scientific journals, including Decision Support Systems, Business & Information Systems Engineering, and Computers & Security.

Vanessa Kohn is a PhD student at Goethe University in Frankfurt, Germany. Her studies focus on digital resilience and sociotechnical systems realignment as well as behavioral information security. Her research has been published in several conference proceedings and scientific journals, including Business & Information Systems Engineering and Journal of Enterprise Information Management.