WHEN COLLEAGUES FAIL: EXAMINING THE ROLE OF INFORMATION SECURITY AWARENESS ON EXTRA-ROLE SECURITY BEHAVIORS

Research paper

Jaeger, Lennart, German Graduate School of Management and Law, Heilbronn, Germany, lennart.jaeger@ggs.de

Eckhardt, Andreas, German Graduate School of Management and Law, Heilbronn, Germany, andreas.eckhardt@ggs.de

Abstract

Although prior information security research predominantly focuses on organizational in-role security behaviors (e.g., information security policy (ISP) compliance), the role of extra-role security behaviors – secure actions unspecified in ISPs but beneficial to organizations – has not seen nearly as much attention. At the same time, employees' awareness manifests itself as prerequisite for security behavior but without research having really understood all of its potential impacts. Therefore this study examines the role of information security awareness (ISA) in enhancing extra-role security behaviors in addition to in-role security behaviors. In particular, we propose that general ISA enhances promotive extra-role security behaviors (i.e., helping and voice) and ISP awareness fosters prohibitive extra-role security behaviors (i.e., stewardship and whistle-blowing). Data was collected from a field study, where employees responded to incoming emails from co-workers and supervisors asking for password sharing, unsafe data sharing via private emails, as well as the use of private cloud services and unauthorized software. Our findings show that general ISA and ISP awareness are indeed driving both in-role and extra-role security behaviors. We discuss our implications for theory and practice, and conclude with interesting avenues for further research.

Keywords: Behavioral security, Extra-role security behaviors, Information security awareness, Information security policy awareness.

1 Introduction

The human factor has become increasingly important in the continuous effort to make business information systems (IS) more secure. In particular, employees have the dual role of being allies and sources of threat to IS security since many security-related incidents are attributed to employees' intentional or unintentional actions (Warkentin and Willison, 2009). Hence, an increasingly critical objective for organizations appears to be both reducing IS threats caused by employees and educating their employees towards becoming secure IS users. A key non-technical measure to achieve this dual objective is to design and implement information security policies (ISPs). ISPs refer to statements of the employees' roles and responsibilities in properly using and protecting organizational IS resources (Bulgurcu et al., 2010). Consequently, ISP compliance and other behaviors specified by or associated with ISPs, subsumed under the term *in-role security behaviors*, have been the primary focus in extant research (e.g., Bulgurcu et al., 2010; Herath and Rao, 2009).

However, recent investigations by Hsu et al. (2015) have pointed out the quixotic act of trying to outline and control every possible security behavior in ISPs and emphasized the importance of *extra-role security behaviors*, which refer to security behaviors not specified in an ISP and not encouraged through rewards or punishments, for ISP effectiveness. Their research implies that an organization's

information security can be further improved, when employees help each other and/or express voice by making innovative suggestions related to ISPs. Following the authors' call to explore other types of extra-role security behaviors and drawing from Van Dyne et al. (1995)'s dimensionality of extra-role behavior, we extend Hsu et al. (2015)'s work on promotive extra-role security behaviors (i.e., helping and voicing) with prohibitive extra-role security behaviors (i.e., stewardship and whistle-blowing). Stewardship and whistle-blowing may be both important for organizational health, because the former protects other colleagues from harm, and the latter places previously undetected problems (e.g., a breach to security by an internal employee) on the organization's agenda to be resolved (Liang et al., 2012). In an information security context, prohibitive behaviors may be possibly more effective than promotive behaviors because, for instance, the process of helping others in learning the right behaviors specified in the ISPs or changing ISPs may require considerable time and effort. Due to ever emerging and frequently changing threats to information security, organization might not be able to afford this luxury. In contrast, stewardship and whistle-blowing call for stopping harm, thereby preventing the negative effects of "process losses" in a timely manner (Liang et al., 2012; Van Dyne et al., 1995).

Yet, in the information security context it is still unclear, who is able and willing to perform these extra-role security behaviors. We argue that it is the employees who are aware of and committed to the security objectives of their organizations, which is commonly referred to as *information security awareness* (ISA) (Siponen, 2000). Users who are committed to the security objectives of their organization, should be more willing to perform activities outside of their regular in-role security behaviors to the benefit of the overall security (Hsu et al., 2015). Thus, our research question is: *How does information security awareness impact extra-role security behaviors?*

We addressed the research question by conducting a field study, where employees were required to read and process business emails (similar to an e-tray exercise). Some of the requests in the emails violated the organization's ISPs, such as requests from colleagues or supervisors asking for password sharing, unsafe data sharing via private emails or private cloud services, and use of unauthorized software. By analyzing screen recordings, we were able to capture employees' actual in-role and extra-role security behaviors in response to these requests.

Before we describe the design and results of our field study in more detail, we will briefly introduce the research background of our work and hypothesize the relationships in our research model. We conclude by discussing our implications for research and practice, along with interesting avenues for further research.

2 Research Background

2.1 Employees' in- and extra-role security behaviors

Behavioral information security research is in broad agreement that to secure information within an organization, appropriate ISPs need to be specified and employees need to be motivated to follow them (Boss et al., 2015; Bulgurcu et al., 2010; Posey et al., 2013). Security activities specified by or associated with ISPs are considered as *in-role security behaviors*, which are required or expected behaviors and are the basis of regular and ongoing job performance (Hsu et al., 2015; Katz, 1964). Examples of in-role security behaviors include among others storing sensitive organizational information only on protected media or locations, protecting one's computer-system account information by never giving it to others, or not using external software unless authorized to do so (Posey et al., 2013). In contrast, *extra-role security behaviors* are discretionary security activities, which are not specified by the ISPs and thus go beyond existing and explicit security-role expectation (Hsu et al., 2015).

In general, extra-role behaviors in organizations are neither formally rewarded when performed nor punished when not performed (Van Dyne and LePine, 1998). Yet, supervisors value extra-role behaviors due to the fact that it is virtually impossible to anticipate and specify all desired employee behaviors. In their literature review of extra-role behaviors in organizations, Van Dyne et al. (1995) proposed a two-dimensional typology, which distinguishes between affiliative/challenging and promo-

tive/prohibitive extra-role behaviors. The first dimension contrasts whether the behavior would likely strengthen or preserve relationships with others (affiliative) or whether it creates a risk of damaging the relationship (challenging). The second dimension contrasts whether the behavior encourages something to occur (promotive) or to cease (prohibitive). Combining these characteristics yields a typology with four general types of extra-role behavior (see Table 1).

	Promotive	**Prohibitive**
Affiliative	Helping	Stewardship
Challenging	Voice	Whistle-blowing

Table 1. A typology of extra-role behaviors (adapted from Van Dyne et al., 1995)

Helping is an example of affiliative promotive behavior, which considers small acts in support of the work of others. It is cooperative behavior which builds and preserves relationships (Van Dyne et al., 1995). This could involve informal assistance in work performance, such as voluntarily taking secure action for coworkers that help to prevent security violations or tips on how to act more securely. *Voice* is an example of challenging promotive behavior, which involves offering comments that may challenge the status quo but do so to improve a situation rather than criticize it (Van Dyne et al., 1995). In the security context, it is making suggestions for change and recommending modifications to ISPs (e.g., on data and password handling or software use). *Stewardship* is an example of affiliative prohibitive behavior, where a more powerful, experienced or skilled employee prohibits or constrains a less powerful, experienced or skilled employee's behavior with the intent of protecting her (Van Dyne et al., 1995). This could involve actively intervening in forbidden or unsecure actions, such as advising colleagues not to use an external cloud service, which may represent a security risk or even a violation of organizational ISPs. *Whistle-blowing* is an example of challenging prohibitive behavior, which is about confronting wrongdoings (Van Dyne et al., 1995). In an information security context, we refer to it as reporting behaviors that are in contravention with the ISPs committed by an internal employee to persons that may be able to effect action (e.g., superiors, information security officers).

We chose to focus on these four extra-role behaviors for two reasons. First, we wanted to build on the theoretical framework developed by Van Dyne et al. (1995), so that our selection of types of extra-role behavior to study would be based on theory rather than on ad hoc criteria. Second, we believed that all four types of extra-role behavior are important in information security. While a recent study has considered promotive extra-role security behaviors (i.e., helping and voicing) (Hsu et al., 2015), to the best of our knowledge, prohibitive extra-role security behaviors have not yet received any attention in information security research.

2.2 Information security awareness

Information security awareness (ISA) is commonly defined as the degree to which employees are aware of and committed to their organization's information security objectives, which is often expressed in organizational ISPs (Siponen, 2000). This understanding of commitment is based on Senge (1994), who regards an organization as a system where its members are not only committed to their own interests, but also to the common interest of the whole . Another way to conceptualize ISA is provided by Dinev and Hu (2007), who define it as an individual's increased consciousness of and interest in knowing about technological issues and strategies to deal with them. Thus, anyone who considers information as a valuable asset, should be aware of possible threats related to it (Siponen, 2001).

Drawing from Siponen's definition, Bulgurcu et al. (2010) additionally differentiate between employees' general knowledge and understanding of security issues and their consequences (termed *general ISA*) as well as their cognizance of their organizations' information security policies and its implications (termed *ISP awareness*) (Bulgurcu et al., 2010). As an illustration, employees may be generally aware that using third-party email systems and storage servers for business tasks is risky (General

ISA) but may not know that the organization requires that information must be secured according to a data protection standard or that users are prohibited from using external providers (ISP awareness).

In prior security research, ISA has been identified as a major driver of varying security behaviors. Previous studies showed that ISA increases employees' ISP compliance (Al-Omari et al., 2012; Bulgurcu et al., 2010; Haeussinger and Kranz, 2013; Putri and Hovav, 2014; Siponen, 2000), adoption of security technologies (Dinev and Hu, 2007; Kumar et al., 2008; Maitland et al., 2012; Han et al., 2014) and desktop security behaviors (White et al., 2017; Hanus and Wu, 2016), as well as decreases access policy violations (Vance et al., 2013), problematic IS security behavior (Takemura, 2011) and IS misuse (D'Arcy et al., 2009; Hovav and D'Arcy, 2012). Departing from prior studies that mainly focused on ISA to investigate in-role security behaviors, we examine whether ISA can promote extra-role security behaviors in addition to in-role security behaviors.

3 Hypotheses Development

3.1 Effect of ISA on in-role security behaviors

Extant research has largely concluded that employees' awareness is one of the most fundamental prerequisites for security behaviors of all kind and in particular plays a key role for employees' in-role security behaviors (Bulgurcu et al., 2010; D'Arcy et al., 2009; Dinev and Hu, 2007; Siponen, 2000). For example, D'Arcy et al. (2009) position awareness as a critical outcome toward ISP compliance, citing its importance for understanding ISPs that govern behavior. In particular, they find that users' awareness of security countermeasures (including ISPs, awareness programs, and computer monitoring) reduces information systems misuse. Employees' awareness of monitoring and evaluation as part of accountability mechanisms was found to reduce their intention to commit ISP violations (Vance et al., 2013). Users' awareness about potential risks and threats of harmful technologies was found to directly determine the intention to use protective information technologies (Dinev and Hu, 2007). Bulgurcu et al. (2010) examined the effect of ISA (consisting of the two dimensions of general ISA and ISP awareness) on employees' ISP compliance. Although their model focused on the effects of three outcome beliefs, it shows a strong positive effect of awareness on employees' compliance attitudes and intentions. By further shedding light on the mediating effect of attitude on the relationship between ISA and compliant intentions, attitude is found only a partial mediator. It is thus reasonable to propose that individuals who are both more cognizant of information security threats (general ISA) and their organization's ISPs (ISP awareness) are more likely to follow them and perform in-role security behaviors. Thus:

Hypothesis 1a: General ISA positively impacts in-role security behaviors.

Hypothesis 1b: ISP awareness positively impacts in-role security behaviors.

3.2 Effect of general ISA on promotive extra-role security behaviors

In collaborative working environments, an employee's work outcomes might by influenced by her coworkers' performance. One member's failing to perform specified ISP behaviors may undermine the department's or even the overall organizational information security (Bachrach et al., 2006). For example, unsafe data sharing or storage among group members can lead to leaking of sensitive information with detrimental consequences for the group or the organization as a whole (e.g., loss of customer trust or lawsuits). This illustration indicates that, when an incident occurs, an employee's organizational environment can be harmed, even when she is not directly responsible for it.

An employee with a high awareness of information security threats and its consequences is at the same time cognizant of the broad consequences of her colleagues' acts on her, other co-workers or the organization as a whole. In this sense, awareness is not mere knowledge but also includes a deeper understanding of interdependencies from a more holistic mind set. She should then have a better under-

standing how she can assist others and avoid interference with her own work (Hsu et al., 2015). That is, when a co-worker asks an individual to perform a task with potentially threatening consequences, highly-aware employees might point employees in the direction of other, more secure alternatives that both support their work and protect the organization. Also having a more comprehensive understanding of security threats and consequences and how formal internal authorities in the organization (e.g. IT department, top management) are dealing with it can lead to helping behavior, if the individual does not have confidence in their acting as being efficient and effective for supporting colleagues and peers.

However, when employees are not able to help their colleagues directly, they need someone with more formal power to deal with the problems they have identified (Detert and Burris, 2007). An "awareness of problems", which is in our context an awareness of information security threats and its consequences, has been found to guide the development of groups that strongly advocate for policies that reduce such problems (Biglan and Taylor, 2000; Dinev and Hu, 2007). An essential step here is to thoroughly articulate the identified problem by extensively communicating to the groups that matter (Biglan and Taylor, 2000). Being aware of information security threats and its consequences (i.e., awareness of problems) drives suggestions from employees to groups that matter to constructively challenge the status quo of information security. Drawing on the illustration above, such suggestions might include innovative solutions on how to handle data sharing or storage.

In conclusion, employees with high levels of general ISA should be more motivated to pay attention to threats to information security in a collaborative context and thus engage in promotive extra-role security behaviors including secure acts in the support of others' work (i.e., helping) and/or speaking up to improve organizational functioning (i.e., voicing). Thus:

Hypothesis 2a: General ISA positively impacts the promotive extra-role security behavior of helping.

Hypothesis 2b: General ISA positively impacts the promotive extra-role security behavior of voice.

3.3 Effect of ISP awareness on prohibitive extra-role security behaviors

ISPs serve as educational tools, because they clarify which behaviors enhance or weaken an organization's information security. Most importantly, they inform employees of their particular role and responsibility in properly using and protecting organization security. They allow employees to understand what they are they are expected to do and further serve as an indicator of the consequences of inappropriate conduct (e.g., formal sanctions) (Bulgurcu et al., 2010; Johnston et al., 2013).

Employees who understand that it is everyone's responsibility to contribute to the overall security of the organization will execute prohibitive influence against inappropriate activities that threaten the organization's information security. When policy-aware employees observe wrongdoings from colleagues who fail to do what is expected of them, they would provide directional instructions intended to stop actions that could cause harm, i.e. they would engage in stewardship behaviors due to a difference in power. Rather than position power or personal power, this difference is based on the more knowledgeable status of the steward compared to the less knowledgeable status of the wrongdoer (Van Dyne et al., 1995). Put differently, the more policy-aware employee directs the less aware employee by trying to constrain his actions with the intent of protecting her and the organization. For example, she could advise her colleague who does not know better not to use unauthorized software, as it is a violation of organizational ISPs.

While employees may be aware of the ISPs, they may lack the position or personal power (French et al., 1968) to enforce them among colleagues. Also, they may have a lack of confidence that their colleagues can solve the problematic behavior and the consequences thereof alone, either because they are not able to due to their lack of awareness or unwilling. In this case, as "law-abiding citizens", policy-aware employees may see it as their duty to safeguard the organization's interest and engage in internal whistle-blowing by reporting wrongdoing to the proper authority (Dozier and Miceli, 1985). For example, policy-aware employees may perceive that their colleagues' unauthorized installation of software or sharing customer data via unsecure channels is wrongful conduct and report it to their su-

perior or security officers to prevent further detrimental consequences and/or prevent problematic behaviors from taking place again.

In conclusion, employees with high levels of ISP awareness should be more motivated to pay attention to ISP violations in a collaborative context and thus engage in prohibitive extra-role security behaviors including constraining colleagues' behavior with the intent of protecting her (i.e., *stewardship*) and/or reporting ISP violations to the proper authority (i.e., *whistleblowing*). Thus we propose:

Hypothesis 3a: ISP awareness positively impacts the prohibitive extra-role security behavior of stewardship.

Hypothesis 3b: ISP awareness positively impacts with the prohibitive extra-role security behavior of whistle-blowing.

Corresponding with prior information security literature we also use *age* and *gender* as control variables for behavior (e.g., D'Arcy et al., 2009). Additionally, we control for the Big Five *personality traits* following extant literature, which established a link between the Big Five personality traits and in-role security behaviors such as ISP compliance (Johnston et al., 2016), as well as on extra-role behaviors (Chiaburu et al., 2011).

4 Research Methodology

To test our hypotheses, we followed a multi-method approach consisting of a field study together with a post-study survey. In the following, we will provide demographic information of our participants, describe our study design, and explain our constructs and measurements.

4.1 Demographics of the participants

Data has been collected from a field study with 107 employees in organizations of 10 sectors, including financial services (n = 57), education (n = 24), manufacturing (n = 7), government (n = 4), energy (n = 3), retail (n = 2), and others (n = 8). Participation was voluntary and anonymous and the employees were told that the purpose of the study is academic research and that independent university scholars would conduct the study and analyze the results. The sample includes 58 men and 49 women, with an average age of 40 years (SD 10 years). In regards to the career status, 43 were administrative clerks, 6 were young professionals (university degree and up to five years job experience), 42 were professionals (university degree and more than five years job experience), 8 had a managing position, and 8 opted out of answering. In terms of the highest level of education, 2 had a PhD, 50 had a master's degree, 6 had a bachelor's degree, 24 were high school graduates, and 22 were secondary school graduates or similar, and 3 opted out of answering. The participants in our sample use a computer at work for 6.55 hours per day on average (SD 2.41), and owns an average of 3.36 email accounts (SD 2.42). Table 2 presents demographic information of the employees in percentage.

Gender	**%**	**Age**	**%**	**Highest level of education**	**%**	**Career status**	**%**
Male	54.2	< 20	1.9	Less than high school degree	20.6	Trainee	0.9
Female	45.8	20-29	8.4	High School degree or similar	22.4	(Administrative) clerk	40.2
		30-39	26.2	Bachelor‘s degree or similar	5.6	Young professional	5.6
		40-49	28.0	Master‘s degree or similar	46.7	Professional	39.3
		50-59	21.5	Doctorate degree	1.9	Manager	7.5
		60-69	4.7	Others	2.8	Others	5.5
		n.s.	9.3				

Table 2. Demographic information of the participants (n=107)

4.2 Study design

The participants were informed that the study's goal is to study human behavior while processing emails and browsing on websites. All participants gave their consent that screen activities on the computer would be recorded during the task. In the consent form, we also emphasized that participation is voluntary and they could withdraw from the study at any stage without penalty, and that data is protected in terms of anonymity and confidentiality. The institutions' data protection officer was consulted and gave her approval prior to the experiments. By recording screen activities, we were able to analyze all behavioral actions and code the in-role and extra-role security behaviors, as described in the next subsection.

Participants received an e-tray exercise similar to other role play scenario experiments (Downs et al., 2006), in which they took the role of an employee at a fictional company, and were required to read and process 20 emails that were stored in the inbox of a webmail server. In order to design our email tasks in our study setting as appropriate as possible for the involved employees, we gathered anonymous examples of internal email exchange within the organizations, where we conducted the field study. For tasks within emails that prompt to access a website with usernames and passwords, usable accounts were provided. Further, files for the study were created and located on the desktop of the computer. A short description of the relationship between the participant and his peers, supervisors, and IT helpdesk was provided, including their names, emails, department, and closeness of the relationship).

For the purpose of this study, the set of emails included nine requests (see Table 3) from six colleagues and three supervisors that violate the ISPs of the participants' organizations, which prescribe storing sensitive corporate information only on protected media or locations (e.g., protected server), no installing of external software on computer unless authorized to do so, no writing down or sharing system login information, among other things.

#	**Subject**	**From**	**Request (summarized)**
1	Trainee applications	Boss	Send two application documents with curriculum vitae for a trainee position to boss's private email.
2	Excel file of existing clients	Peer	Send return on investment calculation file to colleague's private email.
3	New password safe!	Peer	Use the recommended but unauthorized password safe in the attachment (.exe file) for storing passwords.
4	Last meeting protocol?	Peer	Send file of meeting protocol to colleague's private email.
5	Urgent: help with intranet access	Boss	Submit own password to help Boss with a very important and urgent project.
6	Equity finance concept for client	Boss	Send financial plan file for a customer to Boss's private email.
7	Password?	Peer	Send password to a dear colleague in order to quickly help her.
8	Invitation to the Dropbox-Group	Peer	Join Dropbox-Group for Business and upload company-sensitive information and a picture of a team event.
9	Excel list with access	Peer	Share password with work group in excel file because everyone has access to different platforms making collaboration difficult.

Table 3. Features of Emails

4.3 Constructs and measurement

In contrast to and as requested by prior research (e.g., Crossler et al., 2013) we were able to measure participants' actual in-role and extra-role security behaviors. In coding their in-role and extra-role se-

curity behaviors we went through the screen recordings of each participant manually and coded the behavior for each individual email. To establish trustworthiness and credibility of our in-role and extra-role security behavior constructs, we employed principles of data and research triangulation (Lincoln and Guba, 1985). For data triangulation we constantly compared screen-recordings (e.g., email replies) with related definitions and items on in-role and extra-role behaviors. With regard to in-role security behavior, when possible, we drew from Posey et al. (2013)'s taxonomy for protection-motivated behaviors. As an illustration, we considered behavior ID 57 ("*an employee protects his/her computer-system account information by never giving it to other individuals*") and ID1 ("*an employee does not write his/her system login information down*"), when participants were asked to share their password with their supervisor (Email #5), co-worker (Email #7) or the group (Email #9). In coding extra-role security behaviors, we followed Van Dyne et al. (1995)'s typology and contrasted affiliative promotive behaviors (i.e., helping), challenging promotive behaviors (i.e., voice), affiliative prohibitive behaviors (i.e., stewardship), and challenging prohibitive behaviors (i.e., whistleblowing). For research triangulation, two scholars carried out each coding stage independently. We frequently and extensively discussed our coding outcomes, and integrated the coding plans after each coding stage.

In-role security behavior was coded as 1, when a participant did not follow the request in the email by (1) deleting it, (2) archiving it, (3) answering that he cannot follow the request, or (4) not doing anything and moving on to the next email. In contrast, in-role security behavior was coded as 0, when a participant (1) immediately followed the request in the email as asked and thereby violated the organization's ISPs or (2) tried to find some form of workaround they thought would be safer but still violated ISPs (e.g., by answering that they would rather share the password via telephone or encrypting the file but still sending it to a private email account).

Helping behavior was coded as 1, when a participant did not follow the request in the email but took actions in support of the requester's work (Van Dyne et al., 1995). These kind of actions included (1) providing an alternative solution to the request (e.g., sending files to the secure business email instead of the private email, tips to use the organization's private cloud instead of the public cloud, tips to use the organization's authorized password safe instead of the unauthorized one); (2) offering assistance by asking to transfer the needed information via another communication channel (e.g., telephone) or offering to talk on how to handle the request in another way; or (3) providing guidance to the helpdesk or other IT-affine colleagues that could help.

Voice behavior was coded as 1, when participants did not follow the request in the email but provided comments intended to improve the current state to others, such as the supervisor, helpdesk or multiple colleagues. These comments included innovative suggestions for change (Van Dyne et al., 1995). Participants recommended to have a group meeting, jour fixe, or group discussion about (1) how to handle or improve system access and passwords (e.g., use of a password safe, a general department access for emergencies); and (2) how to handle or improve data sharing (e.g., allowing file sharing to a private email when files are encrypted, allowing cloud storage usage or providing an own private cloud).

Stewardship behavior was coded as 1, when a participant did not follow the request in the email but informed the requester she is engaging in behaviors not accepted by organizational ISPs. As opposed to helping, stewardship is characterized by not providing any viable other solutions in support of the work of the requester but is, as per definition, aimed at prohibitive influence against inappropriate activities to avoid harm (Van Dyne et al., 1995).

Whistleblowing behavior was coded as 1, when a participant did not follow the request in the email and reported the request to the appropriate authority (Van Dyne et al., 1995), in our case the supervisor or the IT helpdesk (e.g., "I fear the colleague is doing something reckless. Please inform our CISO so that he points our ISPs out again to him.").

In conclusion, our five latent constructs of in-role behavior, helping, voice, stewardship, and whistleblowing are single-item constructs measured by the mean behavior within the nine emails mentioned in the study design section. Table 4 presents the measurement items for the latent constructs of *general ISA* and *ISP awareness*, which we adopted from Bulgurcu et al. (2010). The Big Five personality traits were used as controls and were measured by the ten-item Big Five Inventory (Rammstedt and John,

2007), which is an abbreviated version of the well-established Big Five Inventory (John et al., 1991). It assesses the Big Five (*Extraversion*, *Agreeableness*, *Conscientiousness*, *Neuroticism*, and *Openness*) with two items per factor, one keyed in the positive and one in the negative direction.

Constructs	**Item**
General ISA	Overall, I am aware of the potential threats to IS security and the protection of sensible data and their negative consequences.
	I have sufficient knowledge about the cost of potential security and privacy problems.
	I understand the concerns regarding information security and privacy and the risks they pose in general.
ISP awareness	I know the rules and regulations prescribed by the information security and privacy policies of my organization.
	I understand the rules and regulations prescribed by the information security and privacy policies of my organization.
	I know my responsibilities as prescribed in the information security and privacy policies to enhance the IS security and privacy of my organization.
Note: All scales ranged from 1 = strongly disagree to 7 = strongly agree.	

Table 4. Measurement Items of Information Security Awareness

5 Analysis and Results

5.1 Measurement model

In our data analysis, we selected the structural equation modelling approach Partial Least Squares (PLS), which is a common regression technique for measuring both measurement and a structural models (Chin, 1998). PLS yields solid results for small to medium sample sizes and can be used to test and validate explanatory models (Chin, 1998). We used the software SmartPLS version 3 for PLS path modelling (Ringle et al., 2015). To assess and evaluate the reflective constructs of the measurement model, their reliability, convergent validity and discriminant validity were analyzed (Fornell and Larcker, 1981; Hair et al., 2006). Table 5 provides the reliability statistics, average variance extracted (AVE), and correlations of the constructs.

	Loadings	**CA**	**CR**	**AVE**	**Correlations**						
					1	2	3	4	5	6	7
General ISA	0.92										
	0.93										
	0.96	0.93	0.96	0.88	**0.94**						
ISP awareness	0.74										
	0.81										
	0.64	0.60	0.77	0.54	0.36	**0.73**					
In-Role	S.I.	S.I.	S.I.	S.I.	0.41	0.42	**S.I.**				
Helping	S.I.	S.I.	S.I.	S.I.	0.20	0.26	0.37	**S.I.**			
Voice	S.I.	S.I.	S.I.	S.I.	-0.12	0.05	-0.10	0.02	**S.I.**		
Stewardship	S.I.	S.I.	S.I.	S.I.	0.21	0.32	0.35	0.22	0.09	**S.I.**	
Whistleblowing	S.I.	S.I.	S.I.	S.I.	-0.02	0.17	0.12	0.06	0.06	0.13	**S.I.**
CA: Cronbach's alpha; CR: composite reliability; AVE: average variance extracted; S.I.: single item. The diagonal elements (in bold) represent the square root of AVE.											

Table 5. Loadings, Cronbach's α, Composite Reliability, Average Variance Extracted, and Correlations

We assessed measurement reliability based on both Cronbach's alpha (CA) and composite reliability (CR). As shown in Table 5, both composite reliability measures exceeded the cutoff values of 0.6. We assessed the convergent and discriminant validity of the reflective constructs using four methods: (1) the square root of the AVE of all constructs were much larger than all other cross-correlations; (2) all AVEs were above 0.50; (3) the correlations among all constructs were below the 0.90 threshold; and (4) all items loaded higher on their intended constructs (cross-loadings can be requested from the authors) (Chin, 1998; Hair et al., 2006). Altogether, these four criteria indicated appropriate convergent and discriminant validity.

5.2 Structural model

The structural model testing results are shown in Figure 1, including estimates of the path coefficients, their significance, and the amount of variances explained (R^2). Based on our hypotheses, we tested the individual impacts of general ISA and ISP awareness on both extra-role and in-role security behaviors. General ISA was found to affect in-role security behavior ($ß$ = 0.259; t = 2.363), promotive extra-role security behavior of helping ($ß$ = 0.246; t = 2.520), but not the promotive extra-role security behavior of voice ($ß$ = -0.104; t = 1.114). ISP awareness was found to affect in-role security behavior ($ß$ = 0.260; t = 2.651), prohibitive extra-role security behavior of stewardship ($ß$ = 0.265; t = 2.920), and whistle-blowing ($ß$ = 0.228; t = 3.185). Hence, with the exception of H2b, all proposed hypotheses were supported. With regard to our control variables, gender, age, and all but one Big Five personality traits were not significant on behaviors. Only employees' voice behavior decreased with the personality trait openness ($ß$ = -0.315, t = 3.014). Furthermore, the combined variance explained by general ISA, ISP awareness and controls was 31.0% for in-role security behavior. General ISA and controls explained 9.0% of variance for helping and 13.0% for voice, whereas ISP awareness and controls explained 14.0% of variance for stewardship and 11.0% for whistle-blowing.

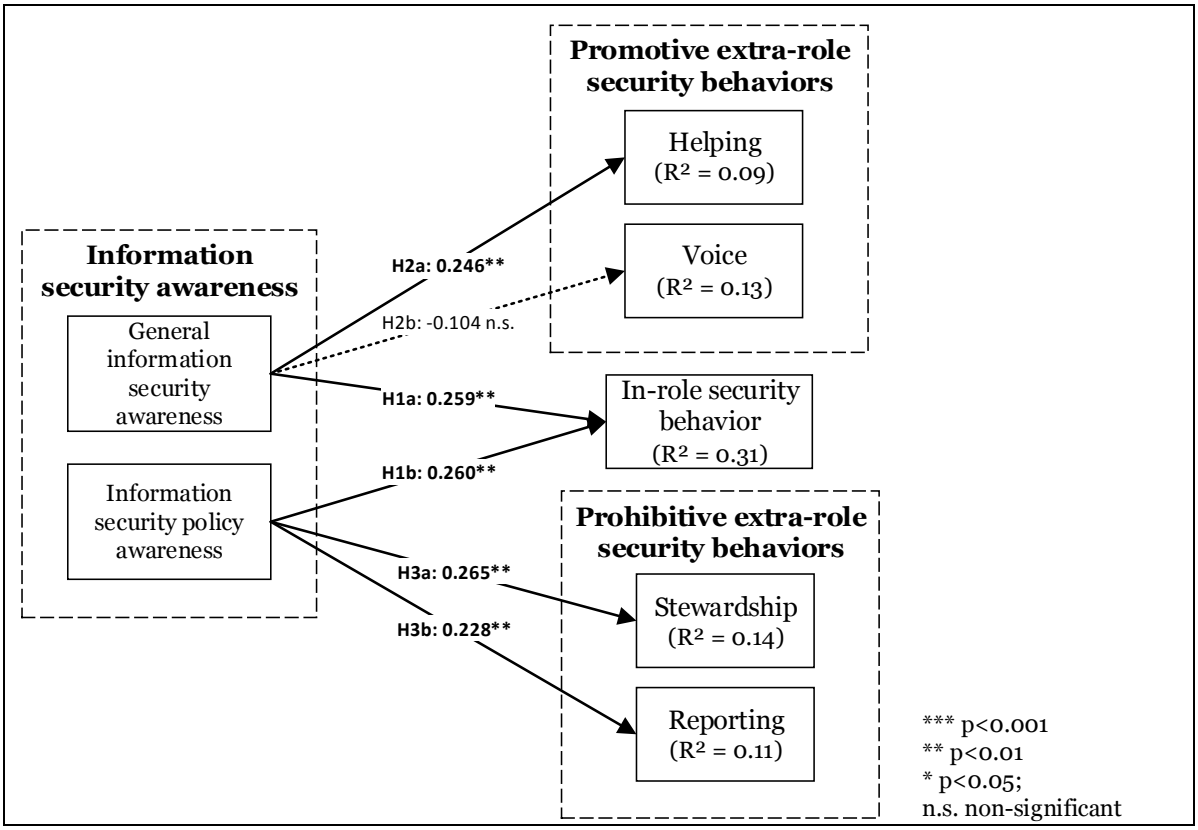

Figure 1. Overall Model Results

6 Discussion

The aim of our study was to determine whether employees' ISA (conceptualized by general ISA and ISP awareness) has an effect on their extra-role security behaviors, on top of their in-role security behaviors. With the help of an elaborated field study, we found that general ISA influences both in-role security behaviors and the promotive extra-role security behavior of helping, but not voicing. Further we found that ISP awareness influences both in-role security behaviors and the prohibitive extra-role security behaviors of stewardship and whistleblowing. Thus, the results largely confirmed our expectation that information security awareness plays also an important role in driving extra-role security behaviors, in addition to in-role security behaviors.

The nonsignificant relationship between general ISA and voice as well as the negative significant relationship between the personality trait openness and voice is contrary to our expectations. Therefore, we revisited the voice literature in search of a potential explanation for these two unexpected results. Several voice theorists (e.g., Detert and Burris, 2007; Detert and Treviño, 2010; Tucker et al., 2008) have argued that management support is a critical contextual influence, because when the receivers (e.g., superiors) send signals that they are not interested in and willing to act on voice, employees' willingness to speak up declines (Detert and Burris, 2007). Thus we tested whether management support moderates the influence of general ISA and openness to change on voice. The rationale is that when employees perceive upper-level support for information security efforts to be absent, employees may be reluctant to voice despite having a high general ISA and being more open to experience. Prior information security researchers have also detailed the importance of management support to accomplishing major tasks and changes with respect to ISP compliance (Hu et al., 2012). The findings of our post hoc analysis (see Appendix) suggest that employees may be reluctant to voice their thoughts despite being aware of problems and being open to experience when they perceive that the receiver is not open to or appreciates information security, and is thus unable or unwilling to respond effectively to voice.

6.1 Implications for research

Our study offers several findings that provide interesting implications to research on information security. As a rising number of (security-aware) employees may find their workplace or organization to be internally threated by their colleagues, there is a need for researchers to explain their behavioral responses to these threats. While extant behavioral research has primarily established that employees' ISA is a major driver of their own in-role security behavior, such as ISP compliance (Bulgurcu et al., 2010), our study extents prior research by introducing awareness as a significant determinant of three extra-role security behaviors, i.e. helping, stewardship, and whistleblowing.

This opens the floor for a debate on how ISA might spread in organizations. When security-aware employees perform affiliative extra-role security behaviors, such as helping or stewardship, to those less aware colleagues, it might have a contagious effect that it in turn also raises their awareness until they are also capable and willing to assist or direct others. However when it comes to challenging extra-role security behaviors, such as voicing and whistleblowing, the felt obligation of security-aware employees for challenging the organization's status quo for a change is, according to our results, rather focused in stopping or preventing harm (i.e., whistle-blowing) than realizing new possibilities (i.e., voicing).

We also extend prior research on extra-role security behavior. In collaborative working environments, employees are actors in a social network, where its performance is determined by the combination of each individual's efforts. Particularly, "weak links" in an organization's information security chain may undermine their organization's security by failing to perform specified ISP behaviors. Thus, it is important to gain an understanding of how these weak links can be reinforced to the degree that ISPs are followed and incidents are reduced. Prior research has established that ISP effectiveness increases when employees help each other and perform voicing behaviors (Hsu et al., 2015), which are both promotive behaviors. We contribute by additionally showing that employees also perform prohibitive

extra-role security behaviors in the form of stewardship and whistleblowing, when they are aware of their organization's ISPs.

Finally, most studies used very static and generic measures for in-role security behavior, like ISP compliance (Bulgurcu et al., 2010; Putri and Hovav, 2014) or ISP violation intentions (D'Arcy et al., 2009; Hovav and D'Arcy, 2012), and extra-role security behavior (Hsu et al., 2015). In our study, we draw from objective and situation-specific behavioral data, i.e. particular behavioral reactions at the moment that a security-related event occurs. This data set provides a rich array of different actions employees may perform in response to potentially threatening requests.

6.2 Implications for practice

This study also offers several implications for practitioners interested in the improvement of organizational information security. First, this research acknowledges that raising both general ISA and ISP awareness is a first step in trying to motivate employees to perform security-related behaviors that are in line with an organization's ISPs. However, organizations should not solely focus on encouraging in-role security behaviors, but should also encourage their employees to perform extra-role security behaviors.

The simultaneous coexistence of different types of employees presents a unique challenge for managers responsible for managing organization-wide information security. Our results could be used as an initial taxonomy that managers can use to identify and classify different security actors in the organization. *Security champions* (high levels of ISA and extra-role security behaviors) are employees who beyond their job description voluntarily take extraordinary interest in information security and could serve as role models of information security. They could influence *security beginners*, i.e., employees who fail to comply due to a lack of awareness (low levels of ISA and in-role security behaviors). Organizations could leverage security champions by pairing them with security beginners in a mentoring program, where the former could provide a one-on-one coaching to the latter and serve as contact person after the coaching.

When practitioners are interested in encouraging promotive extra-role security behaviors our findings indicate that general ISA should be raised. Examples of prominent security breaches that occurred inside the organization (or at another), where one individual's actions affected the whole department or company, could be presented in group meetings or newsletters. As an illustration, a single email sent to a single user with access to group drives can lead to a mass of encrypted data being held for ransom, as was the case in many companies affected by the notorious Locky ransomware attacks (Mathews, 2017). Providing employees with a deeper understanding of interdependencies of how others' actions may also affect them or their own work, should then serve as a motivator to help less capable employees more effectively and securely.

Also if encouraging prohibitive extra-role security behaviors is of interest for practitioners, our findings indicate that, besides general ISA, ISP awareness should be raised as well. Periodic security education, training, and awareness (SETA) programs should strive to have employees recognize the necessity and usefulness of the ISPs' prohibitions and requirements to ensure that employees fully understand their role and responsibility for upholding information security. The key point here is also to convince employees that directing others is wanted as the "strong link" protecting the "weak link" and consequently protecting the organization as a whole. Further, reporting bad behavior is not about pointing the finger at someone but is in the best interest of everyone, as it is about identifying and resolving undetected problems to prevent problematic behaviors from happening again.

6.3 Limitations and future research

When interpreting our results some limitations need to be considered. First, it is difficult to know the extent to which realism was maintained, although we designed our scenario of completing 20 emails in a work environment as realistic and contextually relevant as possible. However, since participants' behavior was recorded, we need to address the issue that participant's in-role and extra-role security

behavior in the study may differ from natural behavior. Second, the process of coding in-role security behaviors and the four extra-role security behaviors was limited to the manual evaluation of screen recordings (all performed actions such as email deletion, archiving, the content of the response emails, actions on the desktop such as opening and installing downloaded files, etc.). Even though we tried to prevent subjectivity while reviewing and coding data, there is still a risk that some of our own biases might have influenced the process. However, we were conscious about that risk and in identifying in-role security behaviors we cross-checked our codings with items identified in Posey et al. (2013)'s taxonomy for protection-motivated behaviors. In coding extra-role security behaviors we focused on the four extra-role behaviors proposed by Van Dyne et al. (1995). Thus, future research could explore other types of extra-role behaviors, such as functional participation, task revision, or principled dissent (Van Dyne et al., 1995). Another interesting avenue to further study employees' sense of responsibility or obligation and its effect on extra-role security behaviors could be to consider the role of psychological ownership. In an organizational context, Van Dyne and Pierce (2004) proposed that psychological ownership would be related to extra-role behaviors. Prior work also suggests that psychological ownership may manifest in differing levels of security behaviors, in particular that ownership may even exert a relatively stronger influence on optional (i.e., extra-role) security behaviors (Anderson and Agarwal, 2010; Thompson et al., 2017). Thus, the model could be further extended by considering the role of psychological ownership for extra-role security behaviors. Third, this research was limited to internal threats related to unsafe data handling (unsecure transfer and storage), password handling (sharing with individuals or a group), and unauthorized software use. Future studies could improve the generalizability of our findings in other settings. Fourth, our sample had a high representation towards financial services staff with fewer participants from other industries. As financial services staff may pay more attention to data protection (due to the nature of the data that they handle, or also due to industry requirements), future research should ensure a more balanced sample between different industries. Last, our field study was geographically confined to Western Europe, thereby potentially neglecting cultural differences. Hence, to generalize the findings, future research is needed to account for cultural differences, for instance with regard to cultural values (e.g., individualism vs. collectivism), which may be of particular interest for multinational organizations.

Appendix

For the post hoc analysis, we split the sample into two groups based on the median of the variable management support (Hu et al., 2012): higher management support (i.e., those that viewed the management "more" supporting with respect to information security), and lower management support (i.e., those that viewed the management "less" supporting with respect to information security). Separate PLS models were run for each subgroup. The results indicate that for the lower management support group, general ISA has a significant negative effect on voice ($ß = -0.263$, $p < 0.05$), but not for the higher management support group ($ß = 0.044$, n.s.). In the same way, for the lower management support group, openness to change has a significant negative effect on voice ($ß = -0.356$, $p < 0.05$), but not for the higher management support group ($ß = -0.228$, n.s.). The findings are discussed in the discussion section.

References

Al-Omari, A., Omar El-Gayar and A. Deokar (2012). "Security policy compliance: User acceptance perspective." In: *Proceedings of the 45th Hawaii International Conference on System Sciences*. Hawaii, Honolulu.

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." *MIS Quarterly* 34 (3), 613–643.

Bachrach, D. G., B. C. Powell, B. J. Collins and R. G. Richey (2006). "Effects of task interdependence on the relationship between helping behavior and group performance." *Journal of Applied Psychology* 91 (6), 1396–1405.

Biglan, A. and T. K. Taylor (2000). "Why have we been more successful in reducing tobacco use than violent crime?" *American Journal of Community Psychology* 28 (3), 269–302.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody and P. Polak (2015). "What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors." *MIS Quarterly* 39 (4), 837–864.

Bulgurcu, B., H. Cavusoglu and I. Benbasat (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly* 34 (3), 523–548.

Chiaburu, D. S., I.-S. Oh, C. M. Berry, N. Li and R. G. Gardner (2011). "The five-factor model of personality traits and organizational citizenship behaviors. A meta-analysis." *Journal of Applied Psychology* 96 (6), 1140–1166.

Chin, W. W. (1998). "The partial least squares approach to structural equation modeling." In: *Modern Methods for Business Research*. Ed. by G. A. Marcoulides. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295–336.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin and R. Baskerville (2013). "Future directions for behavioral information security research." *Computers & Security* 32 (1), 90–101.

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

Detert, J. R. and E. R. Burris (2007). "Leadership Behavior and Employee Voices. Is the Door Really Open?" *Academy of Management Journal* 50 (4), 869–884.

Detert, J. R. and L. K. Treviño (2010). "Speaking up to higher-ups. How supervisors and skip-level leaders influence employee voice." *Organization Science* 21 (1), 249–270.

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

Downs, J. S., M. B. Holbrook and L. F. Cranor (2006). "Decision strategies and susceptibility to phishing." In: *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*. Ed. by L. F. Cranor. New York, New York, USA: ACM Press, p. 79.

Dozier, J. B. and M. P. Miceli (1985). "Potential predictors of whistle-blowing. A prosocial behavior perspective." *Academy of Management Review* 10 (4), 823–836.

Fornell, C. and D. F. Larcker (1981). "Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research* 18 (1), 39–50.

French, J. R. P., B. Raven and D. Cartwright (1968). "The bases of social power." In: *Group Dynamics*. Eds. by D. Cartwright and A. Zander. New York: Harper and Row, pp. 259–269.

Haeussinger, F. and J. Kranz (2013). "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior." In: *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)*. Milan, Italy.

Hair, J. F., W. C. Black, B. J. Babin, R. E. Anderson and R. L. Tatham (2006). *Multivariate data analysis:* Pearson Prentice Hall Upper Saddle River, NJ.

Han, B., Y. Wu and J. Windsor (2014). "User's adoption of free third-party security apps." *Journal of Computer Information Systems* 54 (3), 77–86.

Hanus, B. and Y. Wu (2016). "Impact of Users' Security Awareness on Desktop Security Behavior. A Protection Motivation Theory Perspective." *Information Systems Management* 33 (1), 2–16.

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

Hovav, A. and J. D'Arcy (2012). "Applying an extended model of deterrence across cultures. An investigation of information systems misuse in the U.S. and South Korea." *Information & Management* 49 (2), 99–110.

Hsu, J. S.-C., S.-P. Shih, Y. W. Hung and P. B. Lowry (2015). "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness." *Information Systems Research* 26 (2), 282–300.

Hu, Q., T. Dinev, P. Hart and D. Cooke (2012). "Managing employee compliance with information security policies. The critical role of top management and organizational culture." *Decision Sciences* 43 (4), 615–660.

John, O. P., E. M. Donahue and R. L. Kentle (1991). *The Big Five Inventory- Versions 4a and 54*. Berkeley, CA: University of California, Berkeley, Institute of Personality and Social Research.

Johnston, A. C., M. Warkentin, M. McBride and L. Carter (2016). "Dispositional and situational factors. Influences on information security policy violations." *European Journal of Information Systems* 25 (3), 231–251.

Johnston, A. C., B. Wech and E. Jack (2013). "Engaging Remote Employees. The Moderating Role of "Remote" Status in Determining Employee Information Security Policy Awareness." *Journal of Organizational and End User Computing (JOEUC)* 25 (1), 1–23.

Katz, D. (1964). "The motivational basis of organizational behavior." *Behavioral Science* 9 (2), 131–146.

Kumar, N., K. Mohan and R. Holowczak (2008). "Locking the door but leaving the computer vulnerable. Factors inhibiting home users' adoption of software firewalls." *Decision Support Systems* 46 (1), 254–264.

Liang, J., C. I. C. Farh and J.-L. Farh (2012). "Psychological antecedents of promotive and prohibitive voice. A two-wave examination." *Academy of Management Journal* 55 (1), 71–92.

Lincoln, Y. S. and E. G. Guba (1985). *Naturalistic inquiry*. 3. print. CA, USA: SAGE Publications.

Maitland, C. F., H. F. Thomas and L.-M. N. Tchouakeu (2012). "Internet censorship circumvention technology use in human rights organizations. An exploratory analysis." *Journal of Information Technology* 27 (4), 285–300.

Mathews, L. (2017). *Massive Ransomware Attack Unleashes 23 Million Emails In 24 Hours*. URL: https://www.forbes.com/sites/leemathews/2017/08/31/massive-ransomware-attack-unleashes-23-million-emails-in-24-hours/ (visited on 11/17/2017).

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

Putri, F. F. and A. Hovav (2014). "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory." In: *Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*. Tel Aviv, Israel.

Rammstedt, B. and O. P. John (2007). "Measuring personality in one minute or less. A 10-item short version of the Big Five Inventory in English and German." *Journal of Research in Personality* 41 (1), 203–212.

Ringle, C. M., S. Wende and J.-M. Becker (2015). *SmartPLS 3:* SmartPLS GmbH: Boenningstedt, http://www.smartpls.com.

Senge, P. M. (1994). *The fifth discipline. The art and practice of the learning organization:* Currency Publishing Group, New York.

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

Siponen, M. T. (2001). "Five dimensions of information security awareness." *SIGCAS Computers and Society* 31 (2), 24–29.

Takemura, T. (2011). "Statistical Analysis on Relation between Workers' Information Security Awareness and the Behaviors in Japan." *Journal of Management Policy and Practice* 12 (3), 27.

Thompson, N., T. J. McGill and X. Wang (2017). ""Security begins at home". Determinants of home computer and mobile device security behavior." *Computers & Security* 70, 376–391.

Tucker, S., N. Chmiel, N. Turner, M. S. Hershcovis and C. B. Stride (2008). "Perceived organizational support for safety and employee safety voice. The mediating role of coworker support for safety." *Journal of Occupational Health Psychology* 13 (4), 319.

Van Dyne, L., L. L. Cummings and J. McLean Parks (1995). "Extra-role behaviors: In pursuit of construct and definitional clarity (a bridge over muddied waters)." In: *Research in Organizational Behavior*. Eds. by L. L. Cummings and B. M. Staw. Greenwich: CT: JAI Press, pp. 215–330.

Van Dyne, L. and J. A. LePine (1998). "Helping and voice extra-role behaviors. Evidence of construct and predictive validity." *Academy of Management Journal* 41 (1), 108–119.

Van Dyne, L. and J. L. Pierce (2004). "Psychological ownership and feelings of possession. Three field studies predicting employee attitudes and organizational citizenship behavior." *Journal of Organizational Behavior* 25 (4), 439–459.

Vance, A., P. B. Lowry and D. Eggett (2013). "Using Accountability to Reduce Access Policy Violations in Information Systems." *Journal of Management Information Systems* 29 (4), 263–290.

Warkentin, M. and R. Willison (2009). "Behavioral and policy issues in information systems security: the insider threat." *European Journal of Information Systems* 18 (2), 101–105.

White, G., T. Ekin and L. Visinescu (2017). "Analysis of Protective Behavior and Security Incidents for Home Computers." *Journal of Computer Information Systems* 57 (4), 353–363.