Computers & Security 156 (2025) 104538

Contents lists available at ScienceDirect

Computers & Security

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

Full Length Article

Shadow information security practices in organizations: The role of information security transparency, overload, and psychological empowerment

Duy Dang-Pham [a,*], Nik Thompson [b], Atif Ahmad [c], Sean Maynard [c]

[a] RMIT Vietnam, 702 Nguyen Van Linh Blvd., District 7, Ho Chi Minh City, Vietnam
[b] Curtin University, Kent Street, Bentley, Western Australia, 6102, Australia
[c] The University of Melbourne, Grattan Street, Parkville, Victoria, 3010, Australia

ARTICLE INFO

Keywords:
Information security behavior
Information security management
Shadow security
Psychological empowerment
Security overload
Information security communication

ABSTRACT

Employees are both the first line of defense in organizations and a significant source of vulnerability. Behavioral research in information security (InfoSec) has predominantly studied the compliance of employees with organizational directives. Less understood are 'shadow security practices' – a related category of behavior where employees adopt InfoSec workarounds, albeit to still comply with organizational security needs. We develop a model of the antecedents of employees' intentions to engage in shadow security practices and empirically test our model through a sample of 433 office workers. Results of our structural equation modeling analysis reveal that both *InfoSec overload* and *psychological empowerment* increase intentions to adopt shadow security measures, whereas *perceived transparency of organizational InfoSec* (through InfoSec communication) reduces this intention. Furthermore, we find that these constructs are interrelated and that *InfoSec overload* can be increased by both *psychological empowerment* and *InfoSec transparency*. Our study develops the theoretical understanding of the important yet under-researched concept of shadow security and presents practical recommendations to effectively manage organizational InfoSec through these factors.

1. Introduction

Shadow IT practices, the unsanctioned systems or workarounds created by employees have been the subject of significant attention in recent years. As these practices are neither developed nor controlled by the organizational IT function (Rentrop and Zimmermann, 2012), they may introduce risks for compliance and security efforts (Kopper and Westner, 2016a). As Shadow IT is a broad umbrella concept applied to many areas and applications with different potential impacts (Kopper and Westner, 2016b), it is challenging for researchers to identify the commonalities and themes required to build upon prior work.

One dimension of shadow IT that is potentially impactful includes any information security-related practices or workarounds. Shadow security thus refers to those information security-related practices enacted by employees, especially when they perceive the official practices to be cumbersome (Beris et al., 2015; Kirlappos et al. 2015). Though these employees may be well-intentioned, such actions are essentially a form of non-compliance, or even a new kind of insider threat that extends current classifications (e.g., Prabhu and Thompson, 2020). Though many antecedents of employee compliance have been identified in behavioral studies (Ali et al. 2021; Sommestad et al. 2014), shadow security poses an interesting challenge as it involves behavior that may on the surface appear to be productive and may not be adequately captured by existing constructs.

Any measures that can strengthen the security behaviors of employees have practical relevance as negligent insiders remain one of the most frequent causes of InfoSec incidents and data breaches (EY 2020; KPMG 2020; Verizon 2021). Furthermore, such breaches, even non-volitional or non-malicious, are especially damaging as they often originate in the organization's InfoSec perimeter. There are also associated financial losses caused by non-malicious behaviors such as sharing passwords among colleagues, copying sensitive data to insecure devices or software, and disabling security configurations (Khatib and Barki 2020).

* Corresponding author.
E-mail addresses: duy.dangphamthien@rmit.edu.vn (D. Dang-Pham), nik.thompson@curtin.edu.au (N. Thompson), atif@unimelb.edu.au (A. Ahmad), sean.maynard@unimelb.edu.au (S. Maynard).

https://doi.org/10.1016/j.cose.2025.104538
Received 21 March 2025; Received in revised form 9 May 2025; Accepted 17 May 2025
Available online 20 May 2025

Recognizing the impact of this form of non-malicious InfoSec non-compliance, we study employee motivations for engaging in unsanctioned information security practices. We build upon the body of work in shadow IT to focus on a critical subset of information security related activities known as shadow security (Kirlappos et al. 2014) to develop a structural model of the determinants of such behavior, continuing the work of Dang-Pham et al. (2023). We then collected empirical data from 433 organizational end users and analysed this using structural equation modelling. To the best of our knowledge, we present in this manuscript the first quantitative analysis of the determinants of shadow security behaviors.

Our paper is structured as follows. In the next section, we provide a literature review to define shadow security and identify its potential antecedents, namely perceived InfoSec transparency, InfoSec overload, and psychological empowerment. The following section outlines and explains the rationale for the hypotheses that describe the relationships between these antecedents and shadow security. We then describe our research methods and analysis, followed by a discussion of the findings and contributions. Finally, we conclude our paper by discussing its limitations and providing directions for future research.

2. Literature review

Shadow security refers to unauthorized InfoSec practices that are created and adopted by employees, especially when they perceive official practices to be cumbersome (e.g., related to the management of personal authentication details, information sharing, and personal device usage) (Beris et al. 2015; Kirlappos et al. 2015). A well-established and related concept is shadow IT, which refers to information technology systems deployed or used without explicit approval from the relevant organizational authority (Silic et al. 2017). Whilst the motivations for shadow security and shadow IT alike may align with organizational objectives, the actions of employees utilizing shadow behavior violate organizational policy. For example, a security conscious staff member may be motivated to create backups of important documents but find the corporate SharePoint repository to be awkward or slow to use, leading them to create the backup on their personal portable hard drive. This shadow security workaround is carried out with good intentions; however, it is problematic from a governance and security perspective and is non-compliant with organizational document handling and backup policies.

Traditionally, information security is often treated as a binary decision – employees either comply with the InfoSec policy or they do not (Alotaibi et al. 2017; Kirlappos et al. 2014). Shadow security differs from other noncompliant behaviors in that it consists of actions performed by security-conscious employees (Beris et al. 2015; Kirlappos et al. 2014). These employees consider the organizational need for security when implementing their own InfoSec solutions, and any violations of InfoSec policy are not due to negligence or malicious intention (Beris et al. 2015; Kirlappos et al. 2014). Shadow security is also distinct from shadow IT, as the latter considers the broad use of unauthorized IT solutions to satisfy work requirements without the conscious consideration for organizational InfoSec (Kopper and Westner 2016a; Silic and Back 2014).

2.1. Research motivation

As a unique type of noncompliance, shadow security can open up vulnerabilities and develop a collective false sense of security within the company (Alotaibi et al. 2017; Beris et al. 2015). On the other hand, Kirlappos (et al. 2014) argued that the existence of shadow security behaviors presents a learning opportunity for organizations to reflect on and improve their InfoSec practices. Employees who decide to perform shadow security may consciously want to protect organizational InfoSec, but do so in their own ways. Our research motivation and contributions are thus :

First, understanding the factors that influence shadow security enables organizations to enhance their management of InfoSec, especially to develop a human-centered InfoSec workplace. In the current dynamic security environment, the protection of organizational InfoSec requires not only compliance with policy but also conscious care behaviors (Safa et al. 2015). Organizations also encourage sharing of InfoSec knowledge between employees, and InfoSec champion hubs are recommended for raising awareness within the workplace (Alshaikh 2020; Dang-Pham et al. 2017; Safa and Von Solms 2016). More recently, Wall and Singh (2018) argued that while a compliant persona may be more beneficial for organizational InfoSec under normal operations, employees with an innovative persona can look beyond existing procedures to detect novel threats and solve complex problems such as social engineering more effectively. In this regard, shadow security is performed by employees who are conscious of protecting organizational InfoSec, yet they must creatively find workarounds to satisfy the requirements of both their primary tasks and InfoSec expectations. It is therefore important to identify the reasons that lead to shadow security so that appropriate interventions can be deployed to harness such behavior instead of discouraging it.

Second, shadow security is considered a new and unique type of noncompliance behavior. Stanton et al. (2005) classify InfoSec behaviors according to their level of expertise and intention, which leads to six categories: 1) intentional destruction, 2) detrimental misuse, 3) dangerous tinkering, 4) naïve mistakes, 5) aware assurance, and 6) basic hygiene. Shadow security involves intentional behaviors that violate InfoSec policy, yet the employee also wants to protect organizational InfoSec with their workarounds; thus, it is neither detrimental misuse or careless mistake, nor is it a practice that benefits the organization. Investigating the new shadow security concept offers an opportunity to advance theoretical knowledge by employing existing theoretical frameworks to explain the behavior. Our study aims to contribute to this knowledge gap by examining a conceptual model to identify the antecedents of shadow security. Our central research question is thus:

RQ: What are the antecedents of shadow security intention, and how do these antecedents influence such intention?

2.2. Theoretical foundation

There has been little prior work that has directly addressed the theoretical foundations of shadow security as a construct. However, several theories have been adopted to explain IT-related shadow behaviors at the individual level (Klotz 2019), including Neutralization Theory and the Theory of Workarounds.

Neutralization Theory posits that employees may rationalize to persuade themselves that noncompliance behaviors do not represent a problem (Sykes and Matza 1957). Prior studies have found different types of neutralization techniques, such as the defence of necessity, denial of injury, the metaphor of the ledger, and appeal to higher loyalties (Silic et al. 2017; Siponen and Vance 2010; Willison and Warkentin 2013). For example, when employees feel that they do not have any other choice but to use unauthorized tools to complete their work, they may justify their violation of the IT policy by using such tools as a necessity (Barlow et al. 2013). Employees who violate IT policy believe that their contributions to the organization outweigh the negative consequences caused by using unauthorized technological solutions (Silic et al. 2017).

Recent studies have also employed the Theory of Workarounds to explain employees' justification for their shadow behaviors (Davison and Ou 2017; Khatib and Barki 2020; Silic et al. 2017). According to this theory, workarounds are the goal-driven adaptation of an existing work system to minimize the impact of established constraints and policies that prevent individuals from achieving work effectiveness or other organizational and personal goals (Alter 2014). For example, in the InfoSec context, employees may use their company laptops in public places to complete urgent work or disable InfoSec mechanisms to speed

up the computer (Khatib and Barki 2020). Although these workarounds can be beneficial and productive if they are designed and executed with appropriate knowledge and ethical considerations, they are more likely to create problems as employees do not fully understand the rationale for the existing work systems (Alter 2014).

2.3. Antecedents of shadow security

In their early work in developing the shadow security construct, Kirlappos et al. (2014) suggested that burdensome InfoSec practices were one of the drivers of such behavior. Indeed, high InfoSec overheads, as measured by personal time and cognitive load, have been consistently found to impact both compliance and noncompliance behaviors (Bulgurcu et al. 2010a; Gwebu et al. 2020). In other work, stress and burnout, which are again associated with cumbersome InfoSec requirements, have been shown to lead to noncompliance (D'Arcy, et al. 2014). In situations where there are work goals with competing priorities, employees may feel especially inclined to perform shadow behaviors if they believe such behaviors are necessary for achieving their primary goals and they have the ability to work around the systems (Silic et al. 2017; Siponen and Vance 2010; Sykes and Matza 1957). According to Neutralization Theory and the Theory of Workarounds, the conflicting priorities of primary work and InfoSec tasks are also key factors that lead to the employee performing workarounds and justifying their negligence of InfoSec duties.

Unclear InfoSec communications and perceived gaps in policy have also been identified as prominent causes of shadow security (Kirlappos et al. 2014). Indeed, the quality and quantity of policy-related information have been recognized for their influence on compliance behavior. In the organizational context, the term transparency is used to refer to accurate information disclosure, in which quality and quantity of information are the key conditions to enable the cognitive capabilities of both the sender and the receiver (Albu and Wehmeier 2014; Schnackenberg and Tomlinson 2016). When employees perceive the organization's efforts in providing transparent communication honestly and openly, they feel more confident about their relationship with the organization, thus becoming more likely to express concerns and give feedback to foster organizational changes (Jiang and Luo 2018; Men and Stacks 2014). Similarly, transparent communication promotes the understanding of goals and purposes within the organization, which makes the employees more open to changes (Yue et al. 2019)

Finally, employees' perceptions that their security effort is ignored may also be linked to shadow security behaviors (Kirlappos et al. 2014). Extant literature emphasizes a range of both informal and formal techniques to maintain an adequate InfoSec climate. These include writing an effective InfoSec policy, conducting InfoSec awareness and skills training, social learning, community of practices, and appointment of InfoSec champions (Alshaikh 2020; Alshaikh et al. 2021; Dang-Pham et al. 2017; Paananen et al. 2020; Warkentin et al. 2011). Besides the objective of establishing a shared understanding, these communication techniques also aim to increase employee involvement and engagement in organizational InfoSec activities and discussions (Alshaikh 2020; Karjalainen et al. 2020; Paananen et al. 2020). The employee perceptions that they lack involvement in organizational InfoSec can be mitigated by providing psychological empowerment, which includes security awareness training, access to information, and more participation in InfoSec-related decision making (Dhillon et al. 2020).

In summary, our theoretical explanations for the antecedents of shadow security behaviors identify three factors: 1) Perceived information security transparency, which concerns the quality of InfoSec communication, 2) Information security overload, the state of overload caused by competing expectations of work and InfoSec, and 3) Psychological empowerment, the involvement of the employees in organizational InfoSec activities and discussions. We elaborate on these three constructs in detail in the following sections.

2.3.1. Perceived information security transparency

Perceived InfoSec transparency reflects the quality of InfoSec communication that provides employees with a clear understanding of the operations and outcomes of organizational InfoSec measures (Dang-Pham et al. 2020). Organizational InfoSec is transparent when employees can observe the availability of InfoSec measures, their adoption and usefulness, and why they are recommended by top management. Perceived InfoSec transparency extends the concept of explanation adequacy, which refers to the candid, thorough, reasonable, and timely explanation of security measures by the organization (Lowry et al. 2015). While explanation adequacy focuses on the communication process, perceived InfoSec transparency indicates the quality of the communicated information that enhances the employees' shared understanding of InfoSec measures. Perceived InfoSec transparency is also related to and different from the concept of InfoSec policy quality, which comprises clarity, completeness, and consistency (Bulgurcu et al. 2010b). While InfoSec policy quality focuses on characteristics of the policy, transparency includes perceptions of the quality of information communicated via all mediums and channels within the workplace.

Transparency is essential for building trust between employees and the top management (Schnackenberg and Tomlinson 2016), which in turn increases work efficiency and better standards (Albu and Wehmeier 2014). Nevertheless, excessive communication and transparency can cause disadvantages. First, the large amount of communicated information creates confusion (Yue et al. 2019). Second, giving too much information and explanations may be misinterpreted by employees as the organization is insincere and providing excuses for some hidden agendas (Yue et al. 2019). A balance between too little and too much transparency should be the aim. Similarly, information overload caused by receiving many emails and documentation has also been reported to cause stress and burnout (Kristof-Brown et al. 2005; Sabeeh and Ismail 2013).

2.3.2. Information security overload

InfoSec compliance can be costly (Bulgurcu et al. 2010a; Herath and Rao 2009). Employees may feel that they are overloaded from an InfoSec perspective when they perceive that complying with InfoSec requirements increases their effort when undertaking their primary work tasks (D'Arcy, et al. 2014; Pham 2019). For instance, employees may find that requirements for encrypting company files and using encrypted devices impede their work progress. Cumbersome InfoSec procedures and requirements lead to frustration and stress, and as a consequence, employees may come up with workarounds to circumvent policies and procedures (Beris et al. 2015; Posey, Bennett, and Roberts 2011). Overload can also be caused by information rather than work tasks. Information overload relates to the situation where employees are burdened by a large supply of unsolicited information (Bawden et al. 1999). Similar to work overload, information overload may lead to information anxiety, distraction, poor problem-solving, and making errors at work (Edmunds and Morris 2000; Sabeeh and Ismail 2013). Moreover, employees may ignore relevant information by using filtering strategies to keep the amount of received information at a minimum (Case et al. 2005; Savolainen 2007).

The excessive implementation of InfoSec measures and negative interactions between employees and their workplaces, including constant monitoring that is perceived as an invasion of privacy, can also lead to InfoSec stress and outcomes such as InfoSec misbehaviors (Lee et al. 2016; Posey, Bennett, Roberts, et al. 2011). Characteristics of InfoSec-related information or requirements, such as complexity and uncertainty, also contribute to perceived InfoSec overload (D'Arcy et al. 2014). One of how employees release the feeling of overload is to create workarounds, or shadow security practices, to reduce the time taken on tasks (Kirlappos et al. 2014).

2.3.3. Psychological empowerment

Empowerment takes place when organizations transfer power to

employees through participative management and goal-setting activities so that employees can develop a belief in their authority to make decisions for themselves (Conger and Kanungo 1988). Empowerment programs aim to improve employees' perceptions of work tasks, including the perception of their ability to control, shape, and influence their work environment (Conger and Kanungo 1988; Spreitzer 1995).

The psychological empowerment construct comprises four dimensions that concern the employees' assessment of their (1) competence and (2) autonomy in performing a task, (3) the meaning, and (4) the impact of such a task (Spreitzer 1995). Psychologically empowered employees are confident in their competency, which refers to the belief that they are capable of performing their assigned tasks (Spreitzer 1995). Autonomy or self-determination is about the employees' perception of having the authority and freedom to decide to initiate, control, and continue their work behaviors (Fernandez and Moldogaziev 2015; Spreitzer 1995). Meaning refers to the employees' perception of the task's value, and impact describes the perception of how much the employees' actions can influence organizational outcomes (Conger and Kanungo 1988; Spreitzer 1995).

Psychological empowerment leads to desirable outcomes such as innovation, organizational commitment, and organizational citizenship behavior (Bogler and Somech 2004; Seibert et al. 2011; Shah et al. 2019). Moreover, psychological empowerment may reduce job strain, stress, and turnover intention (Seibert et al. 2011). It is worth noting that psychological empowerment may also result in undesirable outcomes (Mills and Ungson 2003; Spreitzer and Doneson 2005). For example, psychological empowerment might cause employees to believe that they have been given excessive responsibilities, which makes them feel more stressed (Ciulla 1998).

3. Hypothesis development

Previous research has found that perceived response efficacy, or the belief that the InfoSec measures are effective in addressing cybersecurity risks, can motivate compliance (Bulgurcu et al. 2010a; Herath and Rao 2009; Siponen et al. 2014). When employees perceive InfoSec policy to be clear, coherent, and comprehensive, they are more likely to comply with policy directives (Bulgurcu et al. 2010b). Similarly, explanation adequacy was found to reduce reactive computer abuses (Lowry et al. 2015). Employees' understanding of the importance of compliance and the risks of non-compliance, which is reinforced by a clear and well-communicated InfoSec policy, may reduce their intention to carry out InfoSec duties in their own ways (Kirlappos et al. 2015). In our study, perceived InfoSec transparency reflects the employees' understanding of organizational InfoSec measures (Dang-Pham et al. 2020). Thus, we hypothesize that employees will refrain from engaging in shadow security practices when there are effective explanations in the workplace about recommended InfoSec measures, i.e., organizational InfoSec is transparent.

H1: Perceived InfoSec transparency decreases intention to engage in shadow security practices

While information transparency is often the solution for organizational conflicts, too much transparency may decrease the employees' constructive behaviors (De Cremer 2016). An excessively transparent workplace challenges the employees' feelings of autonomy and uniqueness, thereby resulting in undesirable behaviors (De Cremer 2016). When employees receive too much information via different means and channels, such as emails, face-to-face communication, meetings, and promotional materials, they can feel information overload (Bawden et al. 1999; Jackson and Farzaneh 2012; Yue et al. 2019). Similarly, excessive InfoSec-related communication that is complex, difficult to understand, and ambiguous may increase InfoSec overload, which subsequently encourages InfoSec workarounds and computer abuse (D'Arcy et al. 2014; Kirlappos et al. 2014; Pham 2019). It is often desirable to have employees understand organizational InfoSec and recognize InfoSec mechanisms in the workplace, since it motivates employees to comply with InfoSec policy. Nevertheless, we argue that excessive implementation of InfoSec measures, which include intrusive monitoring and an overwhelming number of indicators that constantly remind employees about organizational InfoSec measures being used, may put pressure on employees. Given this, we provide the following hypothesis.

H2: Perceived InfoSec transparency increases InfoSec overload

Transparency was found to motivate positive behaviors such as volunteering for non-task duties, performing work with enthusiasm, helping colleagues, complying with policies and procedures despite their inconvenience, and supporting organizational objectives (Jiang and Luo 2018). Granting employees access to high-quality information sources is a key component of structural empowerment, which leads to a high level of psychological empowerment (Dhillon et al. 2020). We argue that when employees receive adequate information about organizational InfoSec, they are better placed to understand the impact of their InfoSec actions on the organization. Employees will also realize that their InfoSec actions are meaningful and purposeful, thus becoming encouraged to make decisions aligned with the organization's InfoSec goals. We therefore hypothesize:

H3: Perceived InfoSec transparency increases psychological empowerment

Psychological empowerment relates to the decentralization of power among the employees and different managerial levels (Spreitzer 1995). When employees feel psychologically empowered, they perceive InfoSec tasks as personally meaningful and understand that their InfoSec actions can make impactful contributions to the organization (Dhillon et al. 2020). Despite the advantages of psychological empowerment, the mental state of employees has also been found to be associated with negative outcomes such as stress, job strain, and burnout (Laschinger et al. 2001; Seibert et al. 2011). While having power or control may reduce strain (Seibert et al. 2011), empowered employees also feel stress caused by their perceptions of having additional expectations and responsibilities at work (Cheong et al. 2016). When employees perceive that they have greater autonomy thanks to empowerment programs, they may feel frustrated and uncertain about their roles, increasing pressure and reducing work performance (Cheong et al. 2016; Hardy and Leiba-O'Sullivan 1998). We, therefore, propose the following hypothesis:

H4: Psychological empowerment increases InfoSec overload

Psychologically empowered employees feel that they have the autonomy and competence to perform assigned tasks (Spreitzer 1995). We argue that such perceptions of greater autonomy and self-competence may lead to nonroutine or shadow security practices. Prior research found that a high degree of autonomy and self-efficacy, as a result of psychological empowerment, could result in negative organizational outcomes, e.g., causing the kind of uncertainty that makes employees deviate from organizational goals (Mills and Ungson 2003; Spreitzer and Doneson 2005). Likewise, psychologically empowered employees may feel overconfident in their ability to handle InfoSec issues. Therefore, they are more likely to create and adopt shadow security practices that, they believe, improve InfoSec in the organization while allowing them to complete their primary tasks. This is also congruent with Neutralization theory, which posits that employees who violate policies often rationalize that the benefits they bring to the organization outweigh the negative consequences of their actions (Silic et al. 2017).

H5: Psychological empowerment increases the intention to engage in shadow security practices

In our study, InfoSec overload refers to employees' perception of being overburdened with InfoSec duties that add extra pressure and increase their workload (D'Arcy et al. 2014). Prior behavioral InfoSec studies have analyzed the negative outcomes of InfoSec workload, including the increased perceived cost of compliance, burnout, and InfoSec violation (Bulgurcu et al. 2010a; D'Arcy et al. 2014; Pham 2019). Apart from the lack of InfoSec understanding and unavailable compliance mechanisms, high compliance cost was identified as one of the main reasons for employees' non-compliance despite their motivation to protect the organization (Kirlappos et al. 2013). Similarly, the Theory of Workarounds suggests that employees may make work adaptations to minimize the constraints of the work systems and achieve their personal goals (Alter 2014). In line with these arguments, we hypothesize that employees' perception of InfoSec overload encourages them to engage in shadow security practices.

H6: InfoSec overload increases intention to engage in shadow security practices

Fig. 1 illustrates our proposed conceptual model, which is composed of the six hypotheses discussed in this section.

4. Research methods

Structural equation modelling (SEM), which comprises factor analysis and path analysis methods, was employed to examine the proposed conceptual model in Fig. 1. We hired a market research company to collect data using an online survey of office workers. The data collection approach and online survey were reviewed and approved by the ethics committee at the first-named author's institution. At the close of data collection, our final data set contained 433 valid responses.

4.1. Sample

Fifty-five per cent of the respondents were females (238 respondents) and 45 per cent were males (195 respondents). Most of them are 26–35 years old (55.4 per cent), followed by 36–45 (20.3 per cent), 23–25 (17.3 per cent), and 46–35 (6.9 per cent). The majority of the respondents have obtained an undergraduate degree (85.7 per cent), followed by postgraduate degree holders (9.0 per cent), and those who completed high school (5.3 per cent). Our sample primarily consists of full-time employees (87.8 per cent), and 12.2 per cent of the respondents are part-time or casual staff. More than half of these employees work in small and medium companies whose size ranges from 50 to 100 staff (64.5 per cent); other respondents work in larger enterprises with 101–500 employees (18.9 per cent) and with 501 employees and above (16.6 per cent). Our sample also comprises employees who work in diverse industry sectors (see Table 1).

4.2. Survey instrument

Our online questionnaire contained 33 Likert scale items measuring five primary constructs: perceived InfoSec transparency (8 items), psychological empowerment (12 items), InfoSec overload (4 items), and shadow security intention (4 items). These items were adapted from previously validated scales. Another five items were included in the questionnaire to collect data about social desirability bias, which was used for common method bias treatment. We use six-point Likert scales (from "strongly disagree" to "strongly agree") for each of the measurement items to reduce the bias of the survey instrument, by forcing the respondents not to provide "neutral" answers (Garland 1991; Leung 2011). The respondents' gender, tenure year, employment (full-time and part-time), and organization size were also captured by the online questionnaire. Table 2 summarizes the constructs, their definitions, and sources. The measurement items of each construct can be found in the appendix.

5. Analysis

We empirically tested our theoretical model through confirmatory

Table 1
Demographics of sample.

	Frequency (Percent)		Frequency (Percent)
Gender		**Occupation**	
Male	195 (45.0)	Full-time	380 (87.8)
Female	238 (55.0)	Part-time or casual	53 (12.2)
Age		**Company size**	
23–25	75 (17.3)	50 or below 50	219 (50.6)
26–35	240 (55.4)	51–100	60 (13.9)
36–45	88 (20.3)	101–500	82 (18.9)
46–55	30 (6.9)	From 501 and above	72 (16.6)
Education		**Industry**	
High school	23 (5.3)	Retail	59 (13.6)
Undergraduate	371 (85.7)	Education	34 (7.9)
Postgraduate	39 (9.0)	ICT	51 (11.8)
		Healthcare	25 (5.8)
Tenure year		Professional services	57 (13.2)
<5 years	239 (55.2)	Manufacturing	63 (14.5)
From 5 years and above	194 (44.8)	Government	21 (4.8)
		Finance and banking	34 (7.9)
		Other	89 (20.6)

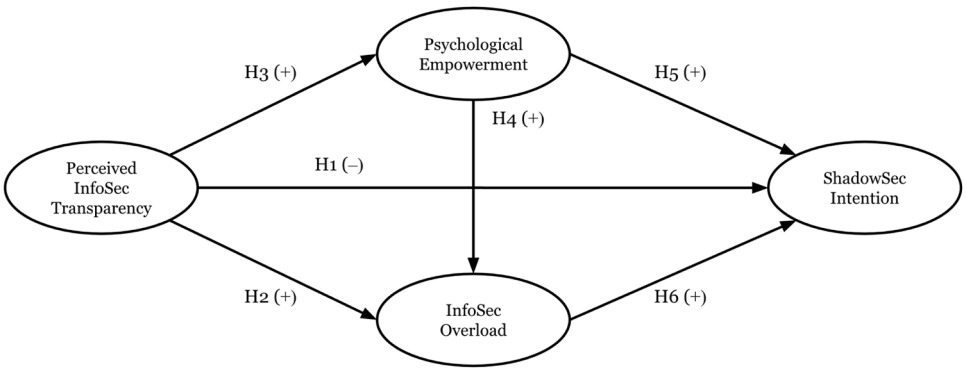

Fig. 1. A conceptual model of the antecedents of shadow security.

Table 2
Constructs, definitions, and sources.

Construct	Definition	References
Perceived InfoSec transparency	The employees' understanding of the operations and outcomes of organizational InfoSec measures which reflects the extent to which InfoSec is clearly communicated within the workplace. The measurement items focus on the employees' understanding of (a) how organizational InfoSec measures are adopted and useful, and (b) why these measures are recommended by the organization.	Dang-Pham et al. (2020)
Psychological empowerment	In our study, psychological empowerment reflects the employees' perceptions of their ability to control, influence, and act on InfoSec-related tasks. Psychological empowerment comprises four dimensions: 1) self-determination, 2) competence, 3) impact, and 4) meaning. Self-determination refers to employees' perception of their autonomy in deciding how they adopt and execute InfoSec tasks. Competence is about the self-belief in having the skills and knowledge to act on the tasks. Impact and meaning refer to the employees' perceptions of how their InfoSec actions are meaningful, important, and able to influence the organization.	Spreitzer (1995)
InfoSec overload	The employees' perception of being burdened and pressured by InfoSec duties that add to their primary work, as a result of excessive InfoSec communication that is complex or ambiguous.	D'Arcy et al. (2014)
Shadow security intention	The employees' intention to engage in shadow security practices - unofficial InfoSec practices that are not recommended by and may be unknown to the organization.	Adapted from Mallmann and Maçada (2021); Silic, Barlow, and Back (2017)

factor analysis (CFA) and structural equation modelling (SEM) by using the IBM SPSS AMOS software (version 24.0.0). During the CFA, we examined the convergent and discriminant validity of the latent variables, i.e., whether the measurement items within a latent variable are correlated with each other, and not with other items outside of their latent variable. The reliability of the latent variables was also assessed.

Theoretical structures of the latent variables followed those that were reported in prior studies. Shadow security intention (SHD), InfoSec overload (OVL), and perceived transparency (TRANS) were specified as first-order constructs. We specified psychological empowerment (PEMP) as a second-order construct which was composed of four dimensions: self-determination (DET), impact (IMP), competence (COMP), and meaning (MEAN), as done by the study providing the original measurement items (Spreitzer 1995). We noted that the phrasing of item SHD2, measuring shadow security intention, might have a situational confounding effect. Nonetheless, as the original definition of shadow security emphasizes the context of shadow security behaviors, where employees cannot follow prescribed InfoSec recommendations (Kirlappos et al., 2014), we decided to keep this item for validity reasons. The standardized factor loading of SHD2 was also 0.675, providing sufficient confidence to retain the item in our model. On the other hand, item OVL4 had a poor factor loading value of <0.5, indicating its lack of association with its latent variable InfoSec overload, and thus necessitated its removal. Our CFA model achieved adequate goodness-of-fit, as evidenced by the following statistics (with acceptance threshold within the parentheses): CMIN/DF=1.880 (between 1 and 3), CFI=0.929 (>0.95), SRMR=0.056 (<0.08), RMSEA=0.045 (<0.06), PCLOSE=0.957 (>0.05).

Table 3 summarizes the set of statistics that satisfied their acceptance thresholds (Hair et al. 2010), and thus indicated good validity and composite reliability (CR) of each latent variable in the CFA model. The statistics suggest that the latent variables are well explained by their measurement items (convergent validity) while being able to distinguish themselves from other variables, i.e., not explained by the items of other latent variables (discriminant validity). The standardized factor loadings of the measurement items can be found in the Appendix. After establishing factor validity and reliability, we proceeded to the next step to detect and address the common method bias within our model.

As our analysis is on self-reported data, we also addressed the risk of common method biases that may influence research results. Besides implementing precautionary means to reduce common method biases, such as mixing the order of questions in the questionnaire and providing clear instructions, we conducted a test to detect social desirability bias in our data. More specifically, the respondents might provide answers to some survey items, especially sensitive ones, in a way that makes them feel socially acceptable. If undetected, social desirability bias can inflate or deflate the impacts of the model's variables on each other, therefore leading to inaccurate interpretations about the variables' relationships.

We performed the zero and constraints tests during the CFA process by including social desirability as an additional latent variable in our model. These tests' results are summarized in Table 4. The p-values of both tests were much smaller than the statistical significance threshold of 0.05, which suggested that (1) social desirability bias existed in the model, and (2) this bias was unevenly distributed among the latent variables. The treatment for such bias was performing imputation to generate factor scores for the latent variables while acknowledging the bias in the respondents' answers, by configuring the social desirability latent variable to affect all measurement items during the imputation.

For the SEM analysis, we specified and evaluated a structural model with the imputed factor scores from the previous CFA step. We also added the employees' gender, company size, tenure year, and employment status (full-time and part-time or casual) to the model as control variables. The structural model achieved excellent goodness-of-fit, as indicated by the following statistics: CMIN/DF=1.165, CFI=0.997, SRMR=0.031, RMSEA=0.020, PCLOSE=0.857. Fig. 2 reports the standardized coefficients of the relationships between the latent variables.

Our model of perceived transparency, psychological empowerment, and InfoSec overload explained 40.4 per cent of the variance in shadow security intention. Perceived transparency was found to decrease the employees' intention to perform shadow security, whereas psychological empowerment and InfoSec overload increased such intention. Furthermore, perceived transparency increased both psychological empowerment and InfoSec overload. InfoSec overload was increased by psychological empowerment. The SEM findings supported all of the proposed hypotheses (Table 5).

The SEM analysis supported our hypothesis that perceived InfoSec transparency reduces shadow security intention. In our study, perceived InfoSec transparency refers to the employees' understanding of how InfoSec measures work, i.e., their operations and outcomes, and why they are recommended by top management (Dang-Pham et al. 2020). As such, a high level of InfoSec transparency reflects effective communication and training about InfoSec in the workplace. Our results on the relationship between perceived transparency and shadow security intention support the view in Kirlappos et al.'s (2014) study that transparent InfoSec communication is necessary for reducing shadow security.

Table 3
Model validity and reliability.

	CR	AVE	MSV	SHD	OVL	PEMP	TRANS
SHD	0.827	0.546	0.236	**0.739**			
OVL	0.751	0.504	0.236	0.486***	**0.710**		
PEMP	0.844	0.579	0.202	0.283***	0.226***	**0.761**	
TRANS	0.916	0.577	0.202	0.063	0.273***	0.449***	**0.760**
Threshold	>0.7	>0.5	<AVE				

Note: CR=composite reliability; AVE=average variance extract; MSV=maximum shared variance; SHD=shadow security intention; OVL=InfoSec overload; PEMP=psychological empowerment; TRANS=perceived InfoSec transparency.

Table 4
Common method bias test results.

	X^2	DF	Delta	p-value
Zero constraints test				
Unconstrained model	1658.185	428	X^2=761.810 DF=27	0.000
Zero constrained model	896.375	455		
Equal constraints test				
Unconstrained model	1658.185	428	X^2=72.781 DF=32	0.000
Equal constrained model	1730.966	454		

Our analysis also confirmed InfoSec overload to be an antecedent of shadow security intention. When employees feel that they cannot comply with the measures prescribed by the organization, they become inclined to perform shadow security in an attempt to protect organizational InfoSec (Kirlappos et al. 2014). There are several reasons why employees might be unable to comply, e.g., unclear instructions or lack of InfoSec skills. InfoSec overload is one of these reasons, and thus our finding of perceived InfoSec overload leading to shadow security intention is congruent with this explanation.

As hypothesized, psychological empowerment was also found to increase shadow security intention. Psychological empowerment is defined as the employee's evaluation of their competence and autonomy in performing InfoSec tasks, as well as the perceived impact and meaning of these tasks (Dhillon et al. 2020). Psychological empowerment can be achieved through InfoSec training and involving employees' participation in InfoSec decision-making processes (Dhillon et al. 2020), which therefore would be anticipated to result in positive organizational outcomes. A meta-analytic review of the consequences of psychological empowerment also mentioned desirable outcomes such as better job satisfaction, organizational commitment, task performance, organizational citizenship behavior, and less job strain and turnover intention (Seibert et al. 2011).

To explain our finding, we suggest that because psychologically empowered employees feel confident in their InfoSec skills and realize the autonomy granted by top management, they perform shadow security while genuinely believing that they are protecting organizational InfoSec. Self-efficacy, as part of the state of being psychologically empowered, has been recognized to potentially produce negative effects, especially when the level of self-efficacy inflates beyond actual capabilities, leading to complacency or overconfidence (Moores and Chang, 2009; Vancouver et al., 2002). In the InfoSec context, Redmiles et al. (2016) found that users who scored lowest on InfoSec tests rated their knowledge as "high", and such miscalibration can lead to not only personal vulnerability but also endanger organizational systems when users in critical positions skip or circumvent InfoSec measures (Greulich et al., 2024; Kumaraguru et al., 2007). Similarly, self-identified InfoSec experts were found to have less secure behaviors than self-identified non-experts, which suggested that self-identified experts might feel empowered to make their own decisions and overlook organizational guidelines (Cain et al. 2018).

The analysis supported our hypotheses concerning the positive effects of perceived InfoSec transparency on psychological empowerment and InfoSec overload. Prior studies on psychological empowerment in general (Seibert et al. 2011) and in the InfoSec context (Dhillon et al. 2020) have identified its antecedents to be contextual factors within an

Table 5
Outcomes of hypothesis testing.

Hypothesis	Description	Test outcome
H1	Perceived InfoSec transparency decreases intention to engage in shadow security practices	Supported
H2	Perceived InfoSec transparency increases InfoSec overload	Supported
H3	Perceived InfoSec transparency increases psychological empowerment	Supported
H4	Psychological empowerment increases InfoSec overload	Supported
H5	Psychological empowerment increases the intention to engage in shadow security practices	Supported
H6	InfoSec overload increases intention to engage in shadow security practices	Supported

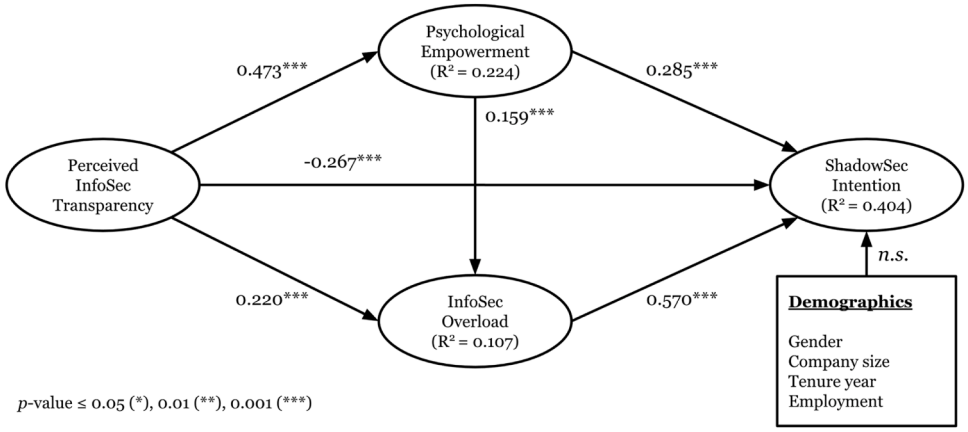

Fig. 2. Structural equation modelling results.

organization and high-performance managerial practices, which include leadership, work design characteristics, participative decision-making, training, and open information sharing. As mentioned above, perceived InfoSec transparency reflects the employees' understanding of InfoSec measures in the workplace that can result from such managerial practices. Consequently, our finding of the positive relationship between perceived InfoSec transparency and psychological empowerment is aligned with current research.

Interestingly, our findings suggested that when employees gain more understanding about InfoSec measures, i.e., perceived InfoSec transparency, they feel more InfoSec overload. Likewise, psychological empowerment was also found to result in InfoSec overload. Prior studies have examined the consequences of InfoSec overload, such as stress, burnout, and policy violation (Lee et al. 2016; Pham 2019), but little is known about its causes. To this end, we contribute to the body of knowledge by identifying perceived InfoSec transparency and psychological empowerment as new antecedents of InfoSec overload for further investigation.

6. Discussion and contributions

InfoSec behaviors have been categorized based on employee intention, ranging from malicious (including misuse and intentional violation) to benevolent (including basic compliance and proactive behaviors) (Stanton et al. 2005). Shadow security falls into the benevolent intention category since the employees performing shadow security want to protect organizational InfoSec, but engage in workarounds, which have potentially detrimental outcomes (Kirlappos et al. 2014). In this research, we aim to identify the antecedents of the employees' intention to perform shadow security, i.e., the InfoSec workarounds that are unofficial and unknown to top management (Kirlappos et al. 2014). Our analysis confirmed quantitatively that perceived InfoSec transparency, psychological empowerment, and InfoSec overload significantly affect the intention to perform shadow security, and we subsequently examined the relationships between these antecedents.

In terms of theoretical contributions, our study expands current knowledge about InfoSec behaviors by identifying the antecedents of the shadow security construct, besides the commonly studied variables such as compliance and noncompliance (Padayachee 2012; Sommestad et al. 2014). To our knowledge, we present the first quantitative research that has operationalized shadow security and empirically determined its antecedents. To this end, we further contribute a set of measurement items to measure shadow security intention, which has been validated with empirical data from the sample of office workers in this study.

In addition to our work on the shadow security construct, our study explored the effects of perceived InfoSec transparency, psychological empowerment, and InfoSec overload, which have not been widely studied by behavioral InfoSec literature. The relationships between these antecedents of shadow security are particularly interesting. While prior studies have highlighted the positive outcomes of InfoSec transparency and psychological empowerment (see e.g., Dhillon et al. 2020; Lowry et al. 2015), we found these factors increase InfoSec overload and subsequently lead to shadow security practices. These findings contradict the common belief that ignorance and confusion are the sole reasons for work overload, and thus empowerment and the provision of sufficient and accurate information about organizational InfoSec to improve transparency reduce InfoSec overload.

The positive effects of perceived InfoSec transparency and psychological empowerment on InfoSec overload suggest various directions for future studies. In particular, mitigations are needed should transparency and psychological empowerment remain the driving factors of InfoSec overload. For instance, future studies may examine the threshold and conditions where InfoSec engagement and empowerment become excessive and result in InfoSec overload. We observed that the number of studies dedicated to enhancing InfoSec initiatives, see e.g., Puhakainen and Siponen (2010), Tsohou et al. (2013), and Spears and Barki (2010), was overshadowed by those that aimed to determine the antecedents of InfoSec behaviors. Thus, we encourage future behavioral research to focus more on *how* organizational initiatives, including SETA training, communication, participative decision-making, and InfoSec task design, should be carried out.

Our findings suggest that increasing the quality of InfoSec engagement and empowerment is more advisable than focusing only on quantity. Excessive InfoSec engagement and empowerment initiatives, including SETA training, frequent communication, and participative decision-making (without thoughtful consideration and follow-up), may further burden employees rather than support them. Organizations should also move beyond simply boosting employees' self-efficacy and make efforts toward calibrating the alignment between perceived and actual capabilities (Moores and Chang, 2009). Calibration-based training that exposes users to practical decision-making scenarios and personalized feedback, as well as adaptive, gamified InfoSec training programs, have been recommended by past studies to reduce cognitive burden and overconfidence, while promoting precaution-taking behaviors (Chen and Koufaris, 2015; Frank, 2020).

Most recently, Greulich et al. (2024) found that trust in organizational protective structures led to reduced personal vigilance, while trust in fair and transparent InfoSec practices resulted in commitment and precaution-taking. They also showed that complacency could suppress security mindfulness, which discouraged precaution-taking. These findings are consistent with ours that perceived InfoSec transparency can reduce shadow security, suggesting that security mindfulness may also discourage shadow security. Organizations are therefore recommended to shift their focus to a balanced InfoSec transparency approach, i.e., prioritizing quality over quantity, emphasizing trust in practices rather than protective structures, to promote InfoSec mindfulness rather than solely increasing employees' self-efficacy. Future InfoSec research is invited to explore the relationship between security mindfulness and shadow security as well.

In line with the above discussions, we also advocate a targeted empowerment approach, where organizations should customize interventions and training programs for specific employee groups. For instance, inflated self-efficacy can result in overplacement, or the belief that one's InfoSec abilities are superior to those of peers, leading to reduced receptivity to training and expert advice, while increasing the tendency to take shortcuts and downplay organizational risks (Ament and Jaeger, 2017; Anderson and Agarwal, 2010; Pennycook et al., 2017). On the other hand, employees with low self-efficacy tend to avoid InfoSec tasks due to fear or perceived difficulty (Liang and Xue, 2009). As such, calibration-based training, focusing on simulations and feedback loops, can be targeted for the former group, whereas the latter may benefit more from scaffolded learning and peer coaching to build foundational confidence. Interestingly, Bachrach et al. (2023) found that perceived proximity, or how close employees feel toward their colleagues and organization, moderates the curvilinear effect of self-efficacy on effort, where high proximity provides social cues that reinforce understanding about effort standards. Similarly, Frank et al. (2023) identified social context, such as team size and communication frequency, as critical predictors of overconfidence. Considering these studies, we recommend that management pay attention to organizational structures when designing and implementing InfoSec interventions. Organizational network analysis methodologies, as demonstrated in the InfoSec context (e.g., Dang-Pham et al., 2017), can offer both practical insights into such structures and inform targeted empowerment interventions, as well as provide opportunities to advance theoretical knowledge through investigating the relationship between organizational structures and shadow security.

7. Limitations and future work

There are certain limitations of this study that need to be noted. First, our findings were drawn from a sample of office workers in Vietnam,

which might be influenced by the country's cultural traits. Employees acting within the information security context adhere to procedures based on shared conventions. These conventions, which may differ from formal organizational policies, are learned through a combination of work experience, environment, professional identity, authority, media, social interactions, cultural values, and organizational culture. (Karjalainen, Siponen, Puhakainen, & Sarker, 2020).

According to Hofstede (2001), the Vietnamese culture has high power distance and collectivism, as well as low uncertainty avoidance, which suggests that Vietnamese people would be more likely to accept organizational hierarchy and prioritize saving face, yet tolerate deviation from the norm more easily. Research has established that power distance, defined as the degree to which members of organizations or institutions accept the legitimacy of unequally distributed power (Hofstede, 1984), impacts job attitudes and can have an effect on counterproductive work behavior (Bochner and Hesketh, 1994). As an employee's power distance orientation can determine how they interpret and respond to authority, there is potential that organizational policy dictated by management may be more readily accepted by those in high power distance cultures.

Our findings indicated that psychological empowerment and InfoSec overload have strong impacts on the employees' intention to perform shadow security, which might be affected by those cultural traits. Specifically, we postulate that when Vietnamese office workers are assigned InfoSec tasks by their managers and receive empowerment, they feel obliged and pressured to perform these tasks so much that they would resort to shadow security workarounds if necessary (this would also apply to countries with similar cultural characteristics to Vietnam such as China and Indonesia). In other cultures that see less importance in the hierarchy and favour uncertainty avoidance more (for example, in Australia or Germany), employees might be more willing to discuss with their managers to find solutions for their InfoSec burdens, and thus they would be less likely to resort to shadow security. To this end, we propose that future work may explore this dimension through cross-cultural replication. As perspectives of certain groups (e.g. IT workers) may differ from those of the national level, we also suggest that work that considers cultural dimensions should do so at the individual level rather than at the national level.

Second, since there has been no prior quantitative research that determined the antecedents of shadow security, there may be other important drivers and inhibitors of shadow security that may extend our conceptual model. For instance, perceptions of the costs and benefits of InfoSec behaviors have been consistently confirmed to be important behavioral antecedents by studies that employed Protection Motivation Theory (Padayachee, 2012; Sommestad et al., 2014). Likewise, both InfoSec compliance and noncompliance are influenced by perceptions of sanctions, according to General Deterrence Theory (D'Arcy and Herath, 2011). Recent work has also empirically demonstrated the link between employee affective responses (e.g., Fear/Concern) and their appraisal of security threats (Thompson and Oldfield, 2024).

Protection Motivation Theory (PMT) (Rogers, 1975) explains that individuals' motivation to address potential threats stems from their evaluation of both the threat and their coping abilities. Originally a model for health behaviors, PMT is now a leading theory in behavioral information systems (IS) security research, a central focus within the IS security field (Boss et al., 2015; Crossler et al., 2013). As such, it has been successfully applied in organizational policy compliance contexts (Vance, Siponen, and Pahnila, 2012), which are comparable to the environment considered in our research. Among key constructs in protection motivation theory are the costs and efficacy of available responses.

Response Efficacy is defined as the conviction that a protective action will be effective in preventing the security threat to oneself or others (Floyd et al., 2000). Response Cost is the perceived cost (e.g., money, time, effort) involved in undertaking the protective action (Floyd, Prentice-Dunn & Rogers, 2000). Both of these have been shown to play a role in employee attitudes towards security (Herath and Rao, 2009). Given that shadow security may be motivated by security requirements being "burdersome" (Beris, Beautement, & Sasse, 2015), it is conceivable that this may be linked to the perceptions of response cost. Future work may integrate established theories in compliance literature, such as PMT, to provide a deeper understanding of shadow security. Similarly, we invite researchers to conduct exploratory and qualitative studies to acquire an in-depth understanding of shadow security and its causes.

8. Conclusion

We found shadow security to be an interesting and practical target variable that should be investigated further by behavioral InfoSec studies. Though shadow IT has been the subject of prior work, this has been around general IT behaviors and not focused on security. However, as security both performs critical tasks and has influence on all other areas of business, we believe it is both intrinsically and positionally important (Dreyfus and Iyer, 2008). Furthermore, given the increasing prevalence of a 'work-from-anywhere mode of activity and the increased connectivity of mobile devices post-pandemic, we anticipate that shadow security will become a key issue as part of the persistent and growing area of insider threats. Studying the motivations and consequences of shadow security thus enables managerial practices to not only correct but also capitalize on these behaviors to improve organizational InfoSec. For instance, practitioners and researchers may examine characteristics of shadow security practices and use them to design InfoSec measures that can be accepted by employees. As such, there is a need for future studies to examine the antecedents and outcomes of shadow security behaviors. We hope that our theoretical model and validated scale instruments provided in this manuscript will enable future researchers to build upon these promising findings.

CRediT authorship contribution statement

Duy Dang-Pham: Writing – original draft, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Nik Thompson:** Writing – review & editing, Writing – original draft, Validation, Project administration. **Atif Ahmad:** Writing – review & editing, Writing – original draft, Validation. **Sean Maynard:** Writing – review & editing, Writing – original draft, Validation.

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.

Appendix A

Table 6.

Table 6
Measurement items and constructs.

Measurement item	Std. factor loading	CR	AVE
Shadow security intention (SHD)		0.827	0.545
SHD1–I intend to use InfoSec measures that I believe are effective, but not prescribed by my company.	0.794		
SHD3–I intend to deploy my own solutions to carry out my InfoSec responsibilities.	0.759		
SHD2–When prescribed InfoSec behavior cannot be followed; I will resort to find other ways to proceed with my primary task.	0.675		
SHD4–I intend to go around InfoSec to comply with the policies in my own way.	0.720		
InfoSec overload (OVL)		0.751	0.504
OVL3–I have a higher workload due to increased information security requirements.	0.725		
OVL1–I am forced by information security policies and procedures to do more work than I can handle.	0.783		
OVL2–My organization's information security policies and procedures hinder my very tight time schedules.	0.612		
OVL4–I am forced to change my work habits to adapt to my organization's information security requirements.	Dropped		
Psychological empowerment (EMP)		0.844	0.579
Self-determination (SFD)	*0.868*	*0.781*	*0.544*
SFD1–I have significant autonomy in determining how I do my job of securing information and information systems.	0.787		
SFD2–I can decide on my own how to go about doing my work of securing information and information systems.	0.699		
SFD3–I have considerable opportunity for independence and freedom in how I do my job of securing information and information systems.	0.723		
Impact (IMP)	*0.809*	*0.791*	*0.558*
IMP1–My impact on what happens in my department related to information security is large.	0.724		
IMP3–I have significant influence over what happens in my department related to information security.	0.766		
IMP2–I have a great deal of control over what happens in my department related to information security.	0.751		
Competence (COMP)	*0.729*	*0.855*	*0.664*
COMP1–I am confident about my ability to do my job of securing information and information systems.	0.826		
COMP3–I have mastered the skills necessary for securing information and information systems.	0.786		
COMP2–I am self-assured about my capabilities to perform my activities in securing information and information systems.	0.831		
Meaning (MEAN)	*0.616*	*0.741*	*0.492*
MEAN1–The work of securing information and information systems is very important to me.	0.611		
MEAN2–The activities of securing information and information systems are personally meaningful to me	0.662		
MEAN3–The work of securing information and information systems is meaningful to me.	0.815		
Perceived InfoSec transparency (TRANS)		0.916	0.577
TRANS1–It is clear and understandable why my company preferred the current InfoSec measures	0.769		
TRANS2–It is clear and understandable why employees are recommended or required to use InfoSec measures in my company	0.802		
TRANS3–It is explained why the recommended InfoSec measures are effective and useful in my company	0.791		
TRANS4–I can tell or it is explained whether the use of InfoSec measures in my company have been effective or not	0.744		
TRANS5–There are visible indicators and mechanisms in my workplace to let employees know whether InfoSec measures are being used properly	0.731		
TRANS6–Overall, decisions and efforts related to organizational InfoSec are transparent, visible and/or clearly communicated	0.770		
TRANS7–It is explained how the recommended InfoSec measures can help to protect computers and information systems in my company	0.805		
TRANS8–I understand the benefits and limitations of the InfoSec measures in my company, as well as the outcomes and impacts that result from its use	0.655		
Threshold	>0.5	>0.7	>0.5

Note: CR = composite reliability; AVE = average variance extracted; bold texts indicate the higher-order latent constructs; italic texts indicate lower-order latent constructs.

Data availability

The authors do not have permission to share data.

References

Albu, O.B., Wehmeier, S., 2014. Organizational transparency and sense-making: the Case of Northern Rock. J. Public Relat. Res. 26 (2), 117–133. https://doi.org/10.1080/1062726X.2013.795869.

Ali, R.F., Dominic, P.D.D., Ali, S.E.A., Rehman, M., Sohail, A., 2021. Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. Appl. Sci. 11 (8). https://doi.org/10.3390/app11083383.

Alotaibi, M., Furnell, S., Clarke, N., 2017. Information Security policies: a review of challenges and influencing factors. In: 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016. Infonomics Society, pp. 352–358. https://doi.org/10.1109/ICITST.2016.7856729.

Alshaikh, M., 2020. Developing cybersecurity culture to influence employee behavior: a practice perspective. Comput. Secur. (98). https://doi.org/10.1016/j.cose.2020.102003.

Alshaikh, M., Maynard, S.B., Ahmad, A., 2021. Applying social marketing to evaluate current security education training and awareness programs in organisations. Comput. Secur. (100), 102090. https://doi.org/10.1016/j.cose.2020.102090.

Alter, S., 2014. Theory of workarounds. Commun. Assoc. Inf. Syst. 34 (55), 1041–1066. http://repository.usfca.edu/at.

Ament, C., Jaeger, L., 2017. Unconscious On Their Own ignorance: Overconfidence in Information Security, 2017. PACIS.

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

Bachrach, D.G., Rapp, T.L., Rapp, A.A., Ogilvie, J., 2023. Too much" self-efficacy? Understanding the curvilinear consequences of between-person self-efficacy through a moderated-mediation model of perceived proximity and employee effort. Group. Organ. Manage 48 (6), 1544–1581.

Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2013. Don't make excuses! discouraging neutralization to reduce IT policy violation. Comput. Secur. (39), 145–159. https://doi.org/10.1016/j.cose.2013.05.006.

Bawden, D., Holtham, C., Courtney, N., 1999. Perspectives on information overload. In: Aslib Proceedings, 51, pp. 249–255. https://doi.org/10.1108/EUM0000000006984.

Beris, O., Beautement, A., Sasse, M.A., 2015. Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors. ACM Int. Conf. Proceeding Ser. 73–84. https://doi.org/10.1145/2841113.2841119), 08-11-Sept.

Bochner, S., Hesketh, B., 1994. Power distance, individualism/collectivism, and job-related attitudes in a culturally diverse work group. J. Cross. Cult. Psychol. 25 (2), 233–257.

Bogler, R., Somech, A., 2004. Influence of teacher empowerment on teachers' Organizational commitment, professional commitment and organizational citizenship behavior in schools. Teach. Teach. Educ. 20 (3), 277–289. https://doi.org/10.1016/j.tate.2004.02.003.

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

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010a. Information security policy compliance: an empirical study on rationality-based beliefs and Information security awareness. MIS. Q. 34 (3), 523–548. https://doi.org/10.2307/25750690.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010b. Quality and fairness of an information security policy as antecedents of employees' Security engagement in the workplace: an empirical investigation. In: Proceedings of the Annual Hawaii International Conference on System Sciences. IEEE, pp. 1–7. https://doi.org/10.1109/hicss.2010.312.

Cain, A.A., Edwards, M.E., Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. (42), 36–45. https://doi.org/10.1016/j.jisa.2018.08.002.
Case, D.O., Andrews, J.E., Johnson, J.D., Allard, S.L., 2005. Avoiding versus seeking: the relationship of information seeking to avoidance, blunting, coping, dissonance, and related concepts. J. Med. Libr. Assoc. 93 (3), 353–362.
Chen, C.W., Koufaris, M., 2015. The impact of decision support system features on user overconfidence and risky behavior. Eur. J. Inf. Syst. 24 (6), 607–623.
Cheong, M., Spain, S.M., Yammarino, F.J., Yun, S., 2016. Two faces of empowering leadership: enabling and burdening. Leadersh. Q. 27 (4), 602–616. https://doi.org/10.1016/j.leaqua.2016.01.006. Elsevier Inc.
Ciulla, J.B., 1998. Leadership and the problem of bogus empowerment. Ethics, The Heart of Leadership. Praeger Publishers, Westport, CT, pp. 63–86. https://doi.org/10.1007/978-3-030-38463-0_12.
Conger, J.A., Kanungo, R.N., 1988. The empowerment process: integrating theory and practice. Acad. Manage Rev. 13 (3), 471–482. https://doi.org/10.5465/amr.1988.4306983.
De Cremer, D., 2016. When transparency backfires, and how to prevent it. Harv. Bus. Rev. Digit. Artic. 2–6.
D'Arcy, J., Herath, T., 2011. A review and analysis of deterrence theory in the IS Security literature: making sense of the disparate findings. Eur. J. Inf. Syst. 20 (6), 643–658. https://doi.org/10.1057/ejis.2011.23.
D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. J. Manage Inf. Syst. 31 (2), 285–318. https://doi.org/10.2753/MIS0742-1222310210.
Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101.
Dang-Pham, D., Hoang, A.-P., Vo, D.-T., Kautz, K., 2020. Explainable information security: development of a construct and instrument. In: The 31st Australasian Conference on Information Systems (ACIS 2020). Wellington, pp. 1–11.
Dang-Pham, D., Pittayachawan, S., Bruno, V., 2017. Applying network analysis to investigate interpersonal influence of information security behaviors in the workplace. Inf. Manage 54 (5), 625–637. https://doi.org/10.1016/j.im.2016.12.003.
Dang-Pham, D., Thompson, N., Ahmad, A., Maynard, S., 2023. Exploring the antecedents of shadow information security practices. In: The 34th Australasian Conference on Information Systems (ACIS 2023). Wellington.
Davison, R.M., Ou, C.X.J., 2017. Digital work in a digitally challenged organization. Inf. Manage 54 (1), 129–137. https://doi.org/10.1016/j.im.2016.05.005. Elsevier B.V.
Dhillon, G., Talib, Y.Y.A., Picoto, W.N., 2020. The mediating role of psychological empowerment in information security compliance intentions. J. Assoc. Inf. Syst. 21 (1), 152–174. https://doi.org/10.17705/1jais.00595.
Dreyfus, D., Iyer, B., 2008. Managing architectural emergence: a conceptual model and simulation. Decis. Support. Syst. 46 (1), 115–127. https://doi.org/10.1016/j.dss.2008.05.004.
Edmunds, A., Morris, A., 2000. Problem of information overload in business organizations: a review of the literature. Int. J. Inf. Manage 20 (1), 17–28. https://doi.org/10.1016/S0268-4012(99)00051-1).
EY. 2020. "EY Global Information Security Survey 2020. How does security evolve from bolted on to built-In?" (https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf).
Fernandez, S., Moldogaziev, T., 2015. Employee empowerment and job satisfaction in the U.S. Federal bureaucracy: a self-determination theory perspective. Am. Rev. Public Adm. 45 (4), 375–401. https://doi.org/10.1177/0275074013507478.
Garland, R., 1991. The mid-point on a rating scale: is it desirable. Mark. Bull. 2 (1), 66–70.
Greulich, M., Lins, S., Pienta, D., Thatcher, J.B., Sunyaev, A., 2024. Exploring contrasting effects of trust in organizational security practices and protective structures on employees' Security-related precaution taking. Inf. Syst. Res. 35 (4), 1586–1608. https://doi.org/10.1287/isre.2021.0528.
Gwebu, K.L., Wang, J., Hu, M.Y., 2020. Information Security Policy noncompliance: an integrative social influence model. Inf. Syst. J. 30 (2), 220–269. https://doi.org/10.1111/isj.12257).
Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2010. Multivariate Data analysis. Multivariate Data Analysis, 7th ed. Prentice Hall, Upper Saddle River, NJ.
Hardy, C., Leiba-O'Sullivan, S., 1998. The power behind empowerment: implications for research and practice. Hum. Relat. 51 (4), 451–483.
Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18 (2), 106–125.
Hofstede, G., 1984. Culture's consequences: International differences in Work-Related Values, 5. Sage.
Hofstede, G., 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, (Second.). Sage Publications, Thousand Oaks CA.
Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30 (2), 407–429.
Frank, M., 2020. Using Calibration to Help Overcome Information Security Overconfidence. ICIS, 2020.
Frank, M., Jaeger, L., Ranft, L.M., 2023. Using contextual factors to predict information security overconfidence: a machine learning approach. Comput. Secur. 125, 103046.
Jackson, T.W., Farzaneh, P., 2012. Theory-based model of factors affecting information overload. Int. J. Inf. Manage 32 (6), 523–532. https://doi.org/10.1016/j.ijinfomgt.2012.04.006.
Jiang, H., Luo, Y., 2018. Crafting employee trust: from authenticity, transparency to engagement. J. Commun. Manag. 22 (2), 138–160. https://doi.org/10.1108/JCOM-07-2016-0055).
Karjalainen, M., Siponen, M., Puhakainen, P., Sarker, S., 2020. Universal and culture-dependent employee compliance of information systems security procedures. J. Glob. Inf. Technol. Manag. 23 (1), 5–24.
Khatib, R., Barki, H., 2020. An activity theory approach to information security non-compliance. Inf. Comput. Secur. 28 (4), 485–501. https://doi.org/10.1108/ICS-11-2018-0128.
Kirlappos, I., Beautement, A., Sasse, M.A., 2013. Comply or die' Is dead: long live security-aware principal agents the need for information security. In: *Financial Cryptography and Data Security* (Vol. 7862 LNCS). Springer Berlin Heidelberg, pp. 70–82. https://doi.org/10.1007/978-3-642-41320-9_5.
Kirlappos, I., Parkin, S., Sasse, M.A., 2014. Learning from 'shadow security': why understanding non-compliant behaviors provides the basis for effective security. In: USEC'14 Workshop on Usable Security.
Kirlappos, I., Parkin, S., Sasse, M.A., 2015. Shadow security' as a tool for the learning organization. ACM SIGCAS Comput. Soc. 45 (1), 29–37. https://doi.org/10.1145/2738210.2738216.
Klotz, S., 2019. Shadow IT and business-managed IT: where is the theory?. In: *Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019* (Vol. 1). IEEE, pp. 286–295. https://doi.org/10.1109/CBI.2019.00039.
Kopper, A., Westner, M., 2016b. Towards a taxonomy for shadow IT. In: Proceedings of AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems, pp. 1–10.
Kopper, A., Westner, M., 2016a. Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature.
KPMG. 2020. "(CS)2 AI-KPMG control system cyber security annual report 2020".
Kristof-Brown, A.L., Zimmerman, R.D., Johnson, E.C., 2005. Consequences of individuals' Fit at work: a meta-analysis of person-job, person-organization, person-group, and person-supervisor FIT. Pers. Psychol. 281–342. https://doi.org/10.1111/j.1744-6570.2005.00672.x.
Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E., 2007. April. Protecting people from phishing: the design and evaluation of an embedded training email system. In: Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 905–914.
Laschinger, H.K.S., Finegan, J., Shamian, J., Wilk, P., 2001. Impact of structural and psychological empowerment on job strain in nursing work settings: expanding Kanter's model. J. Nurs. Adm. 31 (5), 260–272. https://doi.org/10.1097/00005110-200105000-00006.
Lee, C., Lee, C.C., Kim, S., 2016. Understanding information security stress: focusing on the type of information security compliance activity. Comput. Secur. (59), 60–70. https://doi.org/10.1016/j.cose.2016.02.004.
Leung, S.O., 2011. A comparison of psychometric properties and normality in 4-, 5-, 6-, and 11-point likert scales. J Soc v Res 37 (4), 412–421. https://doi.org/10.1080/01488376.2011.580697.
Liang, H., Xue, Y., 2009. Avoidance of information technology threats: a theoretical perspective. MIS. Q. 33 (1), 71–90. https://doi.org/10.2307/20650279.
Lowry, P.B., Posey, C., Bennett, R., Becky, J., Roberts, T.L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. 25 (3), 193–273. https://doi.org/10.1111/isj.12063).
Mallmann, G.L., Maçada, A.C.G., 2021. The mediating role of social presence in the relationship between shadow IT usage and individual performance: a social presence theory perspective. Behav. Inf. Technol. 40 (4), 427–441.
Men, L.R., Stacks, D., 2014. The effects of authentic leadership on strategic internal communication and employee-organization relationships. J. Public Relat. Res. 26 (4), 301–324. https://doi.org/10.1080/1062726X.2014.908720.
Mills, P.K., Ungson, G.R., 2003. Reassessing the limits of structural empowerment: organizational constitution and trust as controls. Acad. Manage Rev. 28 (1), 143–153. https://doi.org/10.5465/AMR.2003.8925254.
Moores, T.T., Chang, J.C.J., 2009. Self-efficacy, overconfidence, and the negative effect on subsequent performance: a field study. Inf. Manage 46 (2), 69–76.
Paananen, H., Lapke, M., Siponen, M., 2020. State of the art in information security policy development. Comput. Secur. (88), 101608. https://doi.org/10.1016/j.cose.2019.101608.
Padayachee, K., 2012. Taxonomy of compliant information security behavior. Comput. Secur. 31 (5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004.
Pennycook, G., Ross, R.M., Koehler, D.J., Fugelsang, J.A., 2017. Dunning–Kruger effects in reasoning: theoretical implications of the failure to recognize incompetence. Psychon. Bull. Rev. 24, 1774–1784.
Pham, H.C., 2019. Information security burnout: identification of sources and mitigating factors from security demands and resources. J. Inf. Secur. Appl. (46), 96–107. https://doi.org/10.1016/j.jisa.2019.03.012.
Prabhu, S., Thompson, N., 2020. A unified classification model of insider threats to information security. In: The 31st Australasian Conference on Information Systems (ACIS 2020). Wellington.
Puhakainen, P., Siponen, M., 2010. Improving employee' compliance through information systems security training: an action research study. MIS. Q. 34 (4), 757–778.
Rentrop, C., Zimmermann, S., 2012. Shadow IT - management and control of unofficial IT. In: Proceedings of the Sixth International Conference on Digital Society.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. j. psychol. 91 (1), 93–114.
Sabeeh, Z.A., Ismail, Z., 2013. Effects of information overload on productivity in enterprises: a literature review. In: *International Conference on Research and Innovation in Information Systems, ICRIIS* (Vol. 2013). IEEE, pp. 210–214. https://doi.org/10.1109/ICRIIS.2013.6716710.

Safa, N.S., Von Solms, R., 2016. An information security knowledge sharing model in organizations. Comput. Hum. Behav. (57), 442–451. https://doi.org/10.1016/j.chb.2015.12.037.

Safa, N.S., Sookhak, M., Solms, R.Von, Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behavior formation in organizations. Comput. Secur. (53), 65–78. https://doi.org/10.1016/j.cose.2015.05.012.

Savolainen, R., 2007. Filtering and withdrawing: strategies for coping with information overload in everyday contexts. J. Inf. Sci. 33 (5), 611–621. https://doi.org/10.1177/0165551506077418.

Schnackenberg, A.K., Tomlinson, E.C., 2016. Organizational transparency: a new perspective on managing trust in organization-stakeholder relationships. J. Manage 42 (7), 1784–1810. https://doi.org/10.1177/0149206314525202.

Seibert, S.E., Wang, G., Courtright, S.H., 2011. Antecedents and consequences of psychological and team empowerment in organizations: a meta-analytic review. J. Appl. Psychol. 96 (5), 981–1003. https://doi.org/10.1037/a0022676.

Shah, T.A., Khattak, M.N., Zolin, R., Shah, S.Z.A., 2019. Psychological empowerment and employee attitudinal outcomes: the pivotal role of Psychological capital. Manag. Res. Rev. 42 (7), 797–817. https://doi.org/10.1108/MRR-05-2018-0194.

Silic, M., Back, A., 2014. Shadow IT – A view from behind the curtain. Comput. Secur. (45), 274–283. https://doi.org/10.1016/j.cose.2014.06.007.

Silic, M., Barlow, J.B., Back, A., 2017. A new perspective on neutralization and deterrence: predicting shadow IT usage. Inf. Manage 54 (8), 1023–1037. https://doi.org/10.1016/j.im.2017.02.007.

Siponen, M., Mahmood, M.A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manage 51 (2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.

Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS. Q. 34 (3), 487–502.

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. https://doi.org/10.1108/IMCS-08-2012-0045.

Spears, J., Barki, H., 2010. User participation in Information systems Security risk management. MIS. Q. 34 (3), 503–522.

Spreitzer, G.M., 1995. Psychological empowerment in the workplace: dimensions, measurement, and validation. Acad. Manage J. 38 (5), 1442–1465.

Spreitzer, G.M., Doneson, D., 2005. Musings on the past and future of employee empowerment. Techno-Struct. Interv. 311–324.

Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., 2005. Analysis of end user security behaviors. Comput. Secur. 24 (2), 124–133.

Sykes, G.M., Matza, D., 1957. Techniques of neutralization: a theory of delinquency. Am. Sociol. Rev. 22 (6), 664. https://doi.org/10.2307/2089195.

Thompson, N., Oldfield, M., 2024. Affective responses to information security threats – the role of threat context and influence on perceived severity. In: 25th Australasian Conference on Information Systems ACIS 2024, Canberra.

Tsohou, A., Karyda, M., Kokalakis, S., Kiontouzis, E., 2013. Managing the introduction of information security awareness programmes in organisations. Eur. J. Inf. Syst. 24 (1), 1–21. https://doi.org/10.1057/ejis.2013.27.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manage 49 (3–4), 190–198.

Vancouver, J.B., Thompson, C.M., Tischner, E.C., Putka, D.J., 2002. Two studies examining the negative effect of self-efficacy on performance. J. Appl. Psychol. 87 (3), 506.

Verizon. 2021. "2021 Data breach investigation report," *DBIR*. (https://doi.org/10.1057/s41280-020-00164-x).

Wall, J.D., Singh, R., 2018. The organization man and the innovator: theoretical archetypes to inform behavioral information security research. DATA BASE Adv. Inf. Syst. 49. April.

Warkentin, M., Johnston, A.C., Shropshire, J., 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur. J. Inf. Syst. 20 (3), 267–284. https://doi.org/10.1057/ejis.2010.72.

Willison, R., Warkentin, M., 2013. Beyond deterrence: an expanded view of employee computer abuse. MIS. Q. 37 (1), 1–20.

Yue, C.A., Men, L.R., Ferguson, M.A., 2019. Bridging transformational leadership, transparent communication, and employee openness to change: the mediating role of trust. Public Relat. Rev. 45 (3), 101779. https://doi.org/10.1016/j.pubrev.2019.04.012.