Association for Information Systems

AIS Electronic Library (AISeL)

ACIS 2023 Proceedings

Australasian (ACIS)

12-2-2023

Exploring the Antecedents of Shadow Information Security Practices

Duy Dang-Pham
RMIT University, Viet Nam, duy.dangphamthien@rmit.edu.vn

Nik Thompson
Curtin University, Australia, nik.thompson@curtin.edu.au

Atif Ahmad
The University of Melbourne, Australia, atif@unimelb.edu.au

Sean Maynard
The University of Melbourne, Australia, sean.maynard@unimelb.edu.au

Follow this and additional works at: https://aisel.aisnet.org/acis2023

Recommended Citation

Dang-Pham, Duy; Thompson, Nik; Ahmad, Atif; and Maynard, Sean, "Exploring the Antecedents of Shadow Information Security Practices" (2023). *ACIS 2023 Proceedings*. 5.
https://aisel.aisnet.org/acis2023/5

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Exploring the Antecedents of Shadow Information Security Practices

Research-in-progress

Duy Dang-Pham
The Business School
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: duy.dangphamthien@rmit.edu.vn

Nik Thompson
School of Management and Marketing
Curtin University
Perth, Australia
Email: nik.thompson@curtin.edu.au

Atif Ahmad
School of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: atif@unimelb.edu.au

Sean Maynard
School of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: sean.maynard@unimelb.edu.au

Abstract

Employees are both the first line of defence in organisations as well as a significant source of vulnerability. Behavioural research in information security (InfoSec) has studied compliance of employees with organisational directives. Less understood are 'shadow security practices'–a related category of behaviour where employees invent InfoSec workarounds albeit with the intention of still complying with organisational InfoSec directives. In this research-in-progress paper, we present the theoretical development of a model, by conducting in-depth reviews of the relevant and multidisciplinary literatures, to identify the potential antecedents of the employees' intention to perform shadow security.

Keywords information security behaviour, information security management, shadow security, information security communication

1 Introduction

Employees are both the first line of defence as well as a significant source of vulnerability (Wall and Singh 2018). Much of the behavioural InfoSec research has determined the motivations for employee compliance with InfoSec directives, which enabled the design and implementation of better initiatives to improve organisational InfoSec (Ali et al. 2021; Sommestad et al. 2014). Nevertheless, negligent insiders are a frequent cause of InfoSec incidents and data breaches (EY 2020; KPMG 2020; Verizon 2021). Security policy breaches, even with no malicious intent, can be most damaging as they are often inside the organisation's InfoSec perimeter. These breaches might include non-malicious behaviours such as sharing of passwords among colleagues, copying sensitive data to insecure devices, and disabling InfoSec configurations (Khatib and Barki 2020), all of which may have a direct financial consequence. Furthermore, prior research has suggested that these non-malicious behaviours may be a precursor to more serious and intentional breaches (Prabhu and Thompson 2020). Non-malicious InfoSec violations are difficult to address, since approaches such as strict policies and excessive sanctions may backfire and lead to intentional sabotage (D'Arcy, Gupta, et al. 2014; Posey, Bennett, Roberts, et al. 2011). Studying these violations thus provides a better understanding of the conflicts and misunderstandings in the workplace that result in these behaviours (Kolkowska et al. 2017). As a unique type of noncompliance, shadow security can open vulnerabilities and create a false sense of security within the company (Alotaibi et al. 2017; Beris et al. 2015). On the other hand, the existence of shadow security behaviours presents a learning opportunity to reflect on and improve InfoSec practices (Kirlappos et al. 2014). Organisational InfoSec can thus be seen as a tension between employees and management (Adams and Sasse 1999; Reinfelder et al. 2019). Employees, who decide to perform shadow security, consciously want to protect organisational InfoSec in their own ways due to difficulty following official InfoSec practices prescribed by management.

Our research motivation and contributions are thus twofold. First, understanding the factors that influence shadow security provides directions for organisations to enhance their InfoSec, especially to develop a human-centered InfoSec workplace. In the current security landscape where threats are dynamically changing, organisational InfoSec requires both compliance and conscious care behaviours (Safa et al. 2015). Wall and Singh (2018) argued that while a compliant persona may be more beneficial for organisational InfoSec under normal operations, employees with an innovative persona can look beyond existing procedure 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 organisational 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 antecedents of shadow security, so that interventions can harness such behaviour instead of discouraging it. Second, shadow security is considered a unique type of noncompliance behaviour that has been under-researched. Shadow security involves intentional behaviours that violate InfoSec policy, yet the employee also wants to protect organisational InfoSec with their workarounds; thus, it is neither detrimental misuse or careless mistake, nor it is a practice that benefits the organisation. Investigating the shadow security concept offers an opportunity to advance theoretical knowledge, by employing existing theoretical frameworks to explain the behaviour. Our research question is:

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

Recognizing the importance of studying non-malicious InfoSec noncompliance, our study puts forward a conceptual model that explains the antecedents of shadow security (Kirlappos et al. 2014). 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 theoretical foundations of the hypotheses which describe the relationships between these antecedents and shadow security. We conclude our paper by discussing its implications and provide directions for future research.

2 Theoretical Foundation

Shadow security refers to unauthorized InfoSec practices that are adopted by employees, especially when they perceive official practices as cumbersome (Beris et al. 2015; Kirlappos et al. 2015). Kirlappos et al. (2014) identified several shadow security practices from their interviews with organizational members, such as copying files to laptops due to insufficient space on network drive or using unencrypted means to share files and deleting the files afterwards due to the lack of a proper tool. Shadow security is related to shadow IT, which refers to information technology systems deployed or used without approval from organisational authority (Silic et al. 2017). Whilst the motivations for shadow security and shadow IT both align with organisational objectives, the actions undertaken by the employees violate organisational policy. Shadow security differs from other noncompliant behaviours in that it consists of workarounds performed by security-conscious employees (Beris et al. 2015; Kirlappos et al. 2014). These employees consider the organisational need for security when coming up with their own solutions for InfoSec issues, e.g., by performing an unauthorized security practice or using an unauthorized software while believing that the performed practice or the software is secure, instead of violating InfoSec policy due to malicious intention (Beris et al. 2015; Kirlappos et al. 2014). Shadow security is also different from shadow IT, as the latter focuses on the use of unauthorized IT solutions to satisfy work requirements without the conscious considerations for organisational InfoSec (Kopper and Westner 2016; Silic and Back 2014).

2.1 Antecedents of shadow security

Shadow security as a new concept has not been explained by any theory-based research. Nonetheless, several theories can explain IT-related shadow behaviours 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 behaviours do not represent a problem (Sykes and Matza 1957). Prior studies have found distinct 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). 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 policy violation as necessity (Barlow et al. 2013). Employees who violate IT policy believe that their positive contributions outweigh the negative consequences caused by using unauthorized technological solutions (Silic et al. 2017). Nevertheless, we found Neutralization Theory insufficient for explaining shadow security, given its focus on the individual's assessment of their behaviours. The larger context of the behaviours, including organisational factors, is not covered by the theory. Therefore, managerial implications derived from the testing of Neutralization Theory are limited.

Recent studies have also employed the Theory of Workarounds to explain employees' justification for their shadow behaviours (Khatib and Barki 2020; Silic et al. 2017). Here, workarounds are the goal-driven adaptation of an existing work system to minimize the impact of established practices, structural constraints and policies that prevent individuals from achieving work effectiveness or other organisational and personal goals (Alter 2014). As such, contextual factors can be the sources of problems that lead to workarounds. 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 policies (Alter 2014). The Theory of Workarounds provide a solid theoretical foundation based on which we could explore further the antecedents of shadow security. First, the definition of shadow security (Beris et al. 2015; Kirlappos et al. 2015) closely matches with that of a workaround. Second, the Theory of Workarounds expands beyond individual's intentions, goals, and interests, and connects these factors to the surrounding structures such as work systems, situational constraints, and routines. With the Theory of Workarounds as a base, we identify the specific antecedents of shadow security by referring to the qualitative study by Kirlappos et al. (2014), from which the concept was originally defined.

Kirlappos et al. (2014) originally proposed the shadow security concept as being caused by burdensome InfoSec practices, mediation within employee teams, and reported security issues that remained unaddressed by management. High InfoSec overheads, as measured by personal time and cognitive load, have been consistently found to impact both compliance and noncompliance behaviours (Bulgurcu et al. 2010a; Gwebu et al. 2020). Studies have also identified InfoSec stress and burnout, which is associated with cumbersome InfoSec requirements, as an important determinant of noncompliance (D'Arcy, Herath, et al. 2014). In situations where there are work goals with competing priorities, employees may feel especially inclined to perform shadow behaviours when able to do so if they believe such behaviours are necessary for achieving their primary goals (Silic et al. 2017; Siponen and Vance 2010; Sykes and Matza 1957). According to Neutralization Theory and the Theory of Workarounds mentioned above, 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.

Kirlappos et al. (2014) suggest that security mediation at team level, or the informal provision of InfoSec instructions and support among employees and managers, encouraged shadow security behaviours. This finding is in line with prior studies which detected the effects of various team-related factors on noncompliance, such as norms, work climate, and social bonds (Cheng et al. 2013; Gwebu et al. 2020).

The empirical network analysis study by (Dang-Pham et al. 2017) detected several social groups of employees who shared InfoSec advice and troubleshooting with each other in the same workplace, which confirmed the high possibility that unofficial InfoSec workarounds could be propagated among employees and managers.

Employees' security effort being ignored is another reason that leads to shadow security behaviours (Kirlappos et al. 2014). This issue also links to the dysfunctional and inconsistent communication about InfoSec within the organisation, resulting in various interpretations of organisational InfoSec requirements and priorities (Kirlappos et al. 2014). The extant literature emphasizes informal and formal communication techniques to maintain an adequate workplace 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). Besides the objective to establish a shared understanding, these techniques also aim to increase the employee involvement and engagement in InfoSec activities and discussions (Karjalainen et al. 2020). The lack of employee involvement in organisational InfoSec, which is evident in their feedback about InfoSec issues being ignored and leads to shadow security (Kirlappos et al. 2014), 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).

Taken together, our explanations for the antecedents of shadow security behaviours identifies three potential factors: 1) the quality of InfoSec communication within the workplace, 2) the state of overload as caused by competing expectations of primary work and InfoSec requirements, and 3) the involvement of the employees in organisational InfoSec activities and discussions. Next, we detail the theoretical constructs related to the three contributing factors of shadow security, namely perceived InfoSec transparency, InfoSec overload, and psychological empowerment.

2.2 Perceived information security transparency

Transparency refers to accurate information disclosure, in which quality and quantity of information are the key conditions to enable cognitive capabilities of both the sender and the receiver (Schnackenberg and Tomlinson 2016). Transparency is important for internal communication as it enhances the employee-organisation relationship, as well as improving trust and corporate reputation (Jiang and Luo 2018). When employees perceive the organisation's efforts in communicating honestly and openly, they feel more confident about their relationship with the organisation, are more likely to express concerns and give feedback to foster organisational changes (Jiang and Luo 2018). Similarly, transparent communication promotes the understanding of goals and purposes within the organisation, which makes the employees more open to changes (Yue et al. 2019).

Perceived InfoSec transparency reflects the quality of communication that provides employees with a clear understanding of the operations and outcomes of organisational InfoSec measures (Dang-Pham et al. 2020). Organisational 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 InfoSec measures by the organisation (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 related though distinct from InfoSec policy quality (Bulgurcu et al. 2010b). While InfoSec policy quality focuses on characteristics of the policy, InfoSec transparency includes perceptions of the quality of information communicated via all mediums and channels within the workplace. Excessive communication and transparency may however have 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 that the organisation 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.

2.3 Information security overload

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, Herath, et al. 2014; Pham 2019). Cumbersome InfoSec procedures and requirements lead to frustration and stress, and as a consequence employees may come up with their own workarounds (Beris et al. 2015; Posey, Bennett, and Roberts 2011). Work overload is defined as the extent to which the performance required in a job exceeds employee expectations (Brown and Benson 2005). Employees also perceive work overload when they receive challenging performance objectives, are assigned too many tasks, or must follow many requirements without sufficient time and resources (Poulose and Dhal 2020). As a result, work overload leads to anxiety, fatigue, burnout, depression, and emotional and psychological stress (Brown and Benson 2005).

Information overload relates to where employees are burdened by a large supply of unsolicited information (Bawden et al. 1999). Similar to work-role overload, information overload may lead to information anxiety, distraction, poor problem-solving, and making errors at work (Sabeeh and Ismail 2013). Moreover, employees may ignore relevant information by using filtering strategies to keep the amount of received information at a minimum (Savolainen 2007). Information overload can lead to conflicts and stress within the work environment (Roetzel 2019).

The excessive implementation of InfoSec measures and negative interactions between employees and their workplaces, including constant monitoring perceived as an invasion of privacy, can also lead to InfoSec stress and outcomes such as InfoSec misbehaviours (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, Herath, et al. 2014). Unclear InfoSec communications and perceived gaps in policy have also been identified as a prominent cause of shadow security (Kirlappos et al. 2014). On the other hand, employees' InfoSec knowledge, perception of threats, adaptation ability, and positive attitude to compliance mitigate InfoSec stress and overload (Lee et al. 2016). One of the ways in which 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).

2.4 Psychological empowerment

Empowerment takes place when organisations transfer power to employees through participative management and goal setting activities, 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). Employee empowerment is often categorized into structural empowerment and psychological empowerment (Conger and Kanungo 1988). While structural empowerment focuses on the managerial practices and arrangements that distribute organisational power among employees, psychological empowerment provides intrinsic motivation to employees who recognize their autonomy and competence (Wagner et al. 2010). Structural empowerment practices can include improving employees' access to information and task conditions, providing opportunities, organisational resources and support (Seibert et al. 2011). By receiving structural empowerment, the employees develop a better understanding of organisational goals and are equipped with the capability and resources necessary for achieving their work goals (Spreitzer 1995).

Structural empowerment is strongly related to psychological empowerment (Dhillon et al. 2020; 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, and (3) the meaning and (4) the impact of such task (Spreitzer 1995). Psychological empowerment leads to desirable outcomes such as innovation, organisational commitment, and organisational citizenship behaviour (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 (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

Prior research has shown that perceived response efficacy, or the employees' belief that the InfoSec measures are effective, 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, reinforced by clear and well-communicated InfoSec policy, may reduce their intentions for noncompliance (Kirlappos et al. 2015). In our study, perceived InfoSec transparency reflects the employees' understanding of the operations and outcomes of organisational InfoSec measures (Dang-Pham et al. 2020). Thus, we hypothesize that employees will refrain from engaging in shadow security practices when there are effective (i.e., transparent) explanations in the workplace about recommended InfoSec measures.

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

While information transparency may resolve organisational conflicts, an excessively transparent workplace challenges the employees' feelings of autonomy and uniqueness, thereby resulting in undesirable behaviours (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; 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, Herath, et al. 2014; Kirlappos et al. 2014; Pham 2019). It is often desirable to have employees understand organisational 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 includes intrusive monitoring and an overwhelming number of indicators that constantly remind employees about organisational InfoSec measures being used, may put pressure on employees. Given this, we provide the following hypothesis.

H2: Perceived InfoSec transparency increases InfoSec overload

Perceived InfoSec transparency relates to employees' understanding of the operations and outcomes of InfoSec measures in the workplace, especially the reasons why InfoSec measures are needed in the workplace (Dang-Pham et al. 2020; Lowry et al. 2015). Transparency was found to motivate positive employees' behaviours such as volunteering for non-task duties, performing work with enthusiasm, helping colleagues, complying with policies and procedures despite their inconvenience, and supporting organisational objectives (Jiang and Luo 2018). Granting employees access to high-quality information sources is a key component of structural empowerment, which leads to an elevated level of psychological empowerment (Dhillon et al. 2020). We argue that when employees receive adequate information about organisational InfoSec, they are better placed to understand the impact of their InfoSec actions on the organisation. Employees will also realize that their InfoSec actions are meaningful and purposeful, thus becoming encouraged to make decisions aligned with the organisation'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 organisation (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 (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). 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 non-routine 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 organisational outcomes, e.g., causing the kind of uncertainty that makes employees deviate from organisational goals (Spreitzer and Doneson 2005). Likewise, psychologically empowered employees may feel over-confident 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 organisation while allowing them to complete their primary tasks. This is also congruent with neutralization theory, which posits that employees, who violate policies, rationalize that the benefits they bring to the organisation 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 burdened with InfoSec duties that add extra pressure and increase their workload, as a result of receiving too much complex or ambiguous InfoSec communication from the company (D'Arcy, Herath, et al. 2014). Prior behavioural InfoSec studies have analysed the negative outcomes of InfoSec workload, including the increased perceived cost of compliance, burnout, and InfoSec violation (Bulgurcu et al. 2010a; D'Arcy, Herath, 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 organisation (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

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

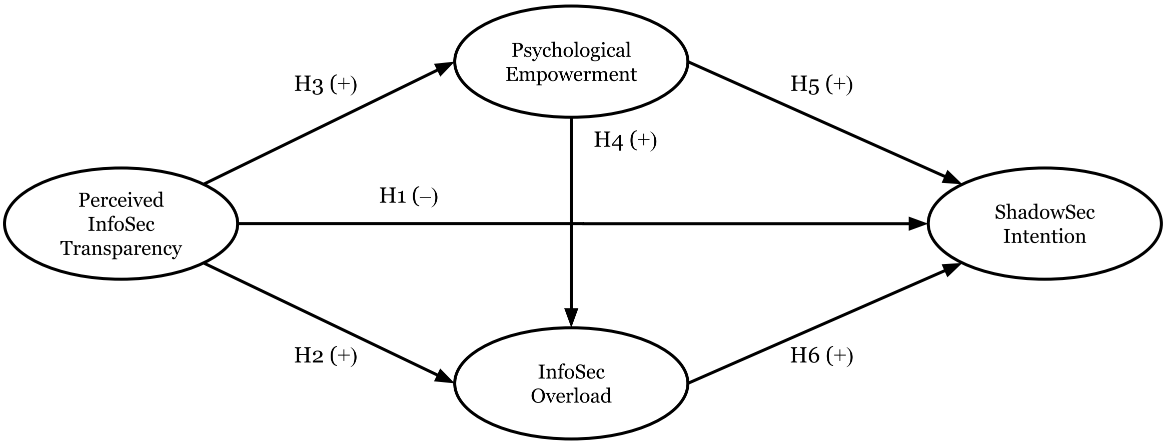

Figure 1. *A conceptual model of the antecedents of shadow security*

4 Conclusion and Future Directions

InfoSec behaviours have been categorized based on employee intention, ranging from malicious (including misuse and intentional violation) to benevolent (including basic compliance and proactive InfoSec behaviours) (Prabhu and Thompson 2020; Stanton et al. 2005). Shadow security falls into the benevolent intention category, since the employees performing shadow security want to protect organisational InfoSec by resorting to workarounds instead of ignoring InfoSec duties, yet the outcomes can be detrimental for organisations (Kirlappos et al. 2014). In this research-in-progress paper we present the development of a model, by conducting reviews of the organizational behavior, management and information systems literatures, to identify the potential 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). This provides a solid foundation from which to continue in several interesting research directions.

The next main step is to move towards empirically testing this proposed model. To this end, the measurement instrument will be finalised. As the constructs in this conceptual model are built from established prior work, it is feasible to adapt validated and tested measures to a considerable extent. However, given that shadow security is an under-researched concept, there may be an opportunity to develop new measurement items. Qualitative studies and thematic analysis may be a valuable approach to developing and refining measures for shadow security. These may then inform the development of a survey instrument suitable for wider distribution and subsequent quantitative analysis using methods such as covariance based/partial least squares (CB/PLS) structural equation modelling (SEM) or fuzzy-set qualitative comparative analysis (fsQCA). As shown in figure 1, perceived InfoSec transparency would reduce shadow security intention, but it would also increase shadow security intention indirectly via psychological empowerment and InfoSec overload. Testing these direct and indirect relationships may shed light on the dual roles of perceived InfoSec transparency, both as a driver and inhibitor of shadow security intention. As the study relates to work practices, data collection must be conducted within the context of an organisation to ensure ecological validity. To this end, the role of national and work cultures may need to be accommodated as this context may have an impact on the findings.

5 References

Adams, A., and Sasse, M. 1999. "Users Are Not the Enemy," *Communications of the ACM* (42:12).

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., and Sohail, A. 2021. “Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance,” *Applied Sciences (Switzerland)* (11:8). (https://doi.org/10.3390/app11083383).

Alotaibi, M., Furnell, S., and Clarke, N. 2017. “Information Security Policies: A Review of Challenges and Influencing Factors,” *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,” *Computers and Security* (98), Elsevier Ltd. (https://doi.org/10.1016/j.cose.2020.102003).

Alshaikh, M., Maynard, S. B., and Ahmad, A. 2021. “Applying Social Marketing to Evaluate Current Security Education Training and Awareness Programs in Organisations,” *Computers and Security* (100), Elsevier Ltd, p. 102090. (https://doi.org/10.1016/j.cose.2020.102090).

Alter, S. 2014. “Theory of Workarounds,” *Communications of the Association for Information Systems* (34:55), pp. 1041–1066.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. “Don’t Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation,” *Computers & Security* (39:PART B), Elsevier Ltd, pp. 145–159. (https://doi.org/10.1016/j.cose.2013.05.006).

Bawden, D., Holtham, C., and Courtney, N. 1999. “Perspectives on Information Overload,” in *Aslib Proceedings* (Vol. 51), pp. 249–255. (https://doi.org/10.1108/EUM0000000006984).

Beris, O., Beautement, A., and Sasse, M. A. 2015. “Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors,” *ACM International Conference Proceeding Series* (08-11-Sept), pp. 73–84. (https://doi.org/10.1145/2841113.2841119).

Bogler, R., and Somech, A. 2004. “Influence of Teacher Empowerment on Teachers’ Organizational Commitment, Professional Commitment and Organizational Citizenship Behavior in Schools,” *Teaching and Teacher Education* (20:3), pp. 277–289. (https://doi.org/10.1016/j.tate.2004.02.003).

Brown, M., and Benson, J. 2005. “Managing to Overload? Work Overload and Performance Appraisal Processes,” *Group and Organization Management* (30:1), pp. 99–124. (https://doi.org/10.1177/1059601104269117).

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010a. “Information Security Policy Compliance: An Empirical Study on Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), pp. 523–548. (https://doi.org/10.2307/25750690).

Bulgurcu, B., Cavusoglu, H., and 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).

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. “Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory,” *Computers & Security* (39), Elsevier Ltd, pp. 447–459.

Cheong, M., Spain, S. M., Yammarino, F. J., and Yun, S. 2016. “Two Faces of Empowering Leadership: Enabling and Burdening,” *Leadership Quarterly* (27:4), Elsevier Inc., pp. 602–616. (https://doi.org/10.1016/j.leaqua.2016.01.006).

Ciulla, J. B. 1998. “Leadership and the Problem of Bogus Empowerment,” in *Ethics, The Heart of Leadership*, Westport, CT: Praeger Publishers, pp. 63–86. (https://doi.org/10.1007/978-3-030-38463-0_12).

Conger, J. A., and Kanungo, R. N. 1988. “The Empowerment Process: Integrating Theory and Practice.,” *Academy of Management Review* (13:3), pp. 471–482. (https://doi.org/10.5465/amr.1988.4306983).

De Cremer, D. 2016. “When Transparency Backfires, and How to Prevent It,” *Harvard Business Review Digital Articles*, pp. 2–6.

Dang-Pham, D., Hoang, A.-P., Vo, D.-T., and 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., and Bruno, V. 2017. "Applying Network Analysis to Investigate Interpersonal Influence of Information Security Behaviours in the Workplace," *Information & Management* (54:5), pp. 625–637. (https://doi.org/10.1016/j.im.2016.12.003).

D'Arcy, J., Gupta, A., Tarafdar, M., and Turel, O. 2014. "Reflecting on the 'Dark Side' of Information Technology Use," *Communications of the Association for Information Systems* (35:July 2014), pp. 109–118. (https://doi.org/10.17705/1cais.03505).

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318. (https://doi.org/10.2753/MIS0742-1222310210).

Dhillon, G., Talib, Y. Y. A., and Picoto, W. N. 2020. "The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions," *Journal of the Association for Information Systems* (21:1), pp. 152–174. (https://doi.org/10.17705/1jais.00595).

EY. 2020. "EY Global Information Security Survey 2020. How Does Security Evolve from Bolted on to Built-In?"

Gwebu, K. L., Wang, J., and Hu, M. Y. 2020. "Information Security Policy Noncompliance: An Integrative Social Influence Model," *Information Systems Journal* (30:2), pp. 220–269. (https://doi.org/10.1111/isj.12257).

Hardy, C., and Leiba-O'Sullivan, S. 1998. "The Power Behind Empowerment: Implications for Research and Practice," *Human Relations* (51:4), pp. 451–483.

Herath, T., and Rao, H. R. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), Elsevier B.V., pp. 154–165. (https://doi.org/http://dx.doi.org/10.1016/j.dss.2009.02.005).

Jiang, H., and Luo, Y. 2018. "Crafting Employee Trust: From Authenticity, Transparency to Engagement," *Journal of Communication Management* (22:2), pp. 138–160. (https://doi.org/10.1108/JCOM-07-2016-0055).

Karjalainen, M., Siponen, M., and Sarker, S. 2020. "Toward a Stage Theory of the Development of Employees' Information Security Behavior," *Computers and Security* (93), Elsevier Ltd, p. 101782. (https://doi.org/10.1016/j.cose.2020.101782).

Khatib, R., and Barki, H. 2020. "An Activity Theory Approach to Information Security Non-Compliance," *Information and Computer Security* (28:4), pp. 485–501. (https://doi.org/10.1108/ICS-11-2018-0128).

Kirlappos, I., Beautement, A., and 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., and 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., and Sasse, M. A. 2015. "'Shadow Security' as a Tool for the Learning Organization," *ACM SIGCAS Computers and Society* (45:1), pp. 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).

Kolkowska, E., Karlsson, F., and Hedström, K. 2017. "Towards Analysing the Rationale of Information Security Non-Compliance: Devising a Value-Based Compliance Analysis Method," *The Journal of Strategic Information Systems* (26:1), The Authors, pp. 39–57. (https://doi.org/10.1016/j.jsis.2016.08.005).

Kopper, A., and Westner, M. 2016. “Towards a Taxonomy for Shadow IT,” in *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, pp. 1–10.

KPMG. 2020. “(CS)2 AI-KPMG Control System Cyber Security Annual Report 2020.”

Lee, C., Lee, C. C., and Kim, S. 2016. “Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity,” *Computers & Security* (59), pp. 60–70. (https://doi.org/http://dx.doi.org/10.1016/j.cose.2016.02.004).

Lowry, P. B., Posey, C., Bennett, R. (Becky) J., and 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,” *Information Systems Journal* (25:3), pp. 193–273. (https://doi.org/10.1111/isj.12063).

Pham, H. C. 2019. “Information Security Burnout: Identification of Sources and Mitigating Factors from Security Demands and Resources,” *Journal of Information Security and Applications* (46), Elsevier Ltd, pp. 96–107. (https://doi.org/10.1016/j.jisa.2019.03.012).

Posey, C., Bennett, R. J., and Roberts, T. L. 2011. “Understanding the Mindset of the Abusive Insider: An Examination of Insiders’ Causal Reasoning Following Internal Security Changes,” *Computers & Security* (30:6–7), Elsevier Ltd, pp. 486–497. (https://doi.org/10.1016/j.cose.2011.05.002).

Posey, C., Bennett, R. J., Roberts, T. L., and Lowry, P. B. 2011. “When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse,” *Journal of Information System Security* (7:1), pp. 24–47.

Poulose, S., and Dhal, M. 2020. “Role of Perceived Work–Life Balance between Work Overload and Career Commitment,” *Journal of Managerial Psychology* (35:3), pp. 169–183. (https://doi.org/10.1108/JMP-03-2018-0117).

Prabhu, S., and Thompson, N. 2020. “A Unified Classification Model of Insider Threats to Information Security,” in *Australasian Conference on Information Systems (ACIS) 2020*, pp. 1–12.

Reinfelder, L., Landwirth, R., and Benenson, Z. 2019. “Security Managers Are Not the Enemy Either,” in *Conference on Human Factors in Computing Systems - Proceedings*, pp. 1–7. (https://doi.org/10.1145/3290605.3300663).

Roetzel, P. G. 2019. “Information Overload in the Information Age: A Review of the Literature from Business Administration, Business Psychology, and Related Disciplines with a Bibliometric Approach and Framework Development,” *Business Research* (12:2), Springer International Publishing, pp. 479–522. (https://doi.org/10.1007/s40685-018-0069-z).

Sabeeh, Z. A., and 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., Sookhak, M., Solms, R. Von, Furnell, S., Ghani, N. A., and Herawan, T. 2015. “Information Security Conscious Care Behaviour Formation in Organizations,” *Computers and Security* (53), Elsevier Ltd, pp. 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,” *Journal of Information Science* (33:5), pp. 611–621. (https://doi.org/10.1177/0165551506077418).

Schnackenberg, A. K., and Tomlinson, E. C. 2016. “Organizational Transparency: A New Perspective on Managing Trust in Organization-Stakeholder Relationships,” *Journal of Management* (42:7), pp. 1784–1810. (https://doi.org/10.1177/0149206314525202).

Seibert, S. E., Wang, G., and Courtright, S. H. 2011. “Antecedents and Consequences of Psychological and Team Empowerment in Organizations: A Meta-Analytic Review,” *Journal of Applied Psychology* (96:5), pp. 981–1003. (https://doi.org/10.1037/a0022676).

Shah, T. A., Khattak, M. N., Zolin, R., and Shah, S. Z. A. 2019. “Psychological Empowerment and Employee Attitudinal Outcomes: The Pivotal Role of Psychological Capital,” *Management Research Review* (42:7), pp. 797–817. (https://doi.org/10.1108/MRR-05-2018-0194).

Silic, M., and Back, A. 2014. “Shadow IT – A View from behind the Curtain,” *Computers & Security* (45), Elsevier Ltd, pp. 274–283. (https://doi.org/10.1016/j.cose.2014.06.007).

Silic, M., Barlow, J. B., and Back, A. 2017. “A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage,” *Information and Management* (54:8), Elsevier B.V., pp. 1023–1037. (https://doi.org/10.1016/j.im.2017.02.007).

Siponen, M., Mahmood, M. A., and Pahnila, S. 2014. “Employees’ Adherence to Information Security Policies: An Exploratory Field Study,” *Information & Management* (51:2), Elsevier B.V., pp. 217–224. (https://doi.org/http://dx.doi.org/10.1016/j.im.2013.08.006).

Siponen, M., and Vance, A. 2010. “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly* (34:3), pp. 487–502.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. “Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies,” *Information Management & Computer Security* (22:1), pp. 42–75. (https://doi.org/10.1108/IMCS-08-2012-0045).

Spreitzer, G. M. 1995. “Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation,” *The Academy of Management Journal* (38:5), pp. 1442–1465.

Spreitzer, G. M., and Doneson, D. 2005. “Musings on the Past and Future of Employee Empowerment,” in *Techno-Structural Interventions*, pp. 311–324.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. “Analysis of End User Security Behaviors,” *Computers & Security* (24:2), pp. 124–133.

Sykes, G. M., and Matza, D. 1957. “Techniques of Neutralization: A Theory of Delinquency,” *American Sociological Review* (22:6), p. 664. (https://doi.org/10.2307/2089195).

Verizon. 2021. “2021 Data Breach Investigation Report,” *DBIR*. (https://doi.org/10.1057/s41280-020-00164-x).

Wagner, J. I. J., Cummings, G., Smith, D. L., Olson, J., Anderson, L., and Warren, S. 2010. “The Relationship between Structural Empowerment and Psychological Empowerment for Nurses: A Systematic Review,” *Journal of Nursing Management* (18:4), pp. 448–462. (https://doi.org/10.1111/j.1365-2834.2010.01088.x).

Wall, J. D., and Singh, R. 2018. “The Organization Man and the Innovator: Theoretical Archetypes to Inform Behavioral Information Security Research,” *The DATA BASE for Advances in Information Systems* (49:April).

Yue, C. A., Men, L. R., and Ferguson, M. A. 2019. “Bridging Transformational Leadership, Transparent Communication, and Employee Openness to Change: The Mediating Role of Trust,” *Public Relations Review* (45:3), Elsevier, p. 101779. (https://doi.org/10.1016/j.pubrev.2019.04.012).

Copyright

Copyright © 2023 Dang-Pham, Thompson, Ahmad, Maynard. This is an open-access article licensed under a Creative Commons Attribution-Non-Commercial 3.0 Australia License, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and ACIS are credited.