ISSN 0144-929X

Volume 38 Number 5 May 2019

Behaviour & Information Technology

An international journal on the human aspects of computing

Editor-in-Chief
Panos Markopoulos

Taylor & Francis
Taylor & Francis Group

Taylor & Francis
Taylor & Francis Group

Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

# Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation

Ying Li, Nan Zhang & Mikko Siponen

**To cite this article:** Ying Li, Nan Zhang & Mikko Siponen (2019) Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation, Behaviour & Information Technology, 38:5, 435-453, DOI: 10.1080/0144929X.2018.1539519

**To link to this article:** https://doi.org/10.1080/0144929X.2018.1539519

Published online: 25 Oct 2018.

BEHAVIOUR & INFORMATION TECHNOLOGY
2019, VOL. 38, NO. 5, 435–453
https://doi.org/10.1080/0144929X.2018.1539519

Taylor & Francis
Taylor & Francis Group

# Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation

Ying Li[a], Nan Zhang[b] and Mikko Siponen[c]

[a]Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, P.R. People's Republic of China; [b]School of Management, Harbin Institute of Technology, Harbin, Heilongjiang, P.R. People's Republic of China; [c]Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland

**ABSTRACT**

Employees' violation of information security policies is a major threat to an organisation. Some violations such as using an easy-to-guess password or storing confidential data on personal unencrypted flash drives usually do not cause immediate harm; instead, these actions create security flaws that can be attacked in the future and cause delayed consequences. We call such behaviour consequence-delayed information security violation (CDISV). The ignorance or denial of the possible delayed consequences is the main reason employees engage in such insecure behaviour. Due to the delay between the action and the consequence, a long-term mindset could play an important role in employees' current decision-making. Specifically, in this study, we propose that long-term orientation is an influential factor in decreasing CDISV. The long-term orientation includes three dimensions: continuity, futurity, and perseverance. In addition, based on the stewardship theory and the needs theory, we further propose that value identification and the fulfilment of higher-order needs (trusted relationship and growth) are important drivers for employees to have a long-term orientation. We collected survey data using the 170 responses we received from a global company's employees. The empirical results support our arguments. Our findings provide implications to organisations to encourage employees' information security behaviours.

**ARTICLE HISTORY**
Received 26 March 2018
Accepted 15 October 2018

**KEYWORDS**
Information security behaviour; consequence-delayed information security violation; long-term orientation; higher-order needs; stewardship theory

## 1. Introduction

Humans often create security weaknesses and flaws in information systems (IS), which is a critical threat to an organisation's IS. A recent report indicated that 30% of data breaches are caused by trusted but negligent insiders, which ranked second only to malware as the most serious threat to organisations' information security (Ponemon 2015). Similarly, in another report, 73% of the selected companies rated employee errors and omissions as top threats to organisations (Deloitte 2013). The results from Ponemon Institute's recent report revealed that all types of insider threats are increasing. Since 2016, the average number of incidents involving employee or contractor negligence has increased from 10.5 to 13.4 for an organisation, and the average annualized cost of insider-related incidents has reached to $3.8 million (Ponemon 2018a). In another Ponemon institute's report, the per capita cost of a data breach due to human errors or negligence was $128 (Ponemon 2018b). These findings indicate that human errors in security incidents cause tremendous economic cost to organisations. In addition, European Union's General Data Protection Regulation (GDPR) comes into force in 2018, which urges organisations to better train their employees to be fully aware of the everyday security risks. Because, the data breach incidents could cost a lot more than just information. If a company is found to be in breach of GDPR, it will be subject to fines of 4% of its annual global turnover or €20 million. To sum up, insider threat has been going as an organisation's major concern.

Among the various forms of insider threats, a particular type of behaviour threat occurs quite often—the behaviour that does not cause immediate consequences but leaves vulnerability to the IS. For instance, selecting an easy-to-guess password may not cause an immediate data breach, or even a few minutes afterwards (as a fire would), but continuing to use it may increase the risk of getting hacked, and lead to a data breach in the end. For another example, storing an organisation's confidential data in an employee's unauthorised USB stick may not lead to an instant disclosure of data. However, with the accumulation of time, the risk of data breach is increasing. In one case, the USB stick may fall into the

**CONTACT** Ying Li ✉ yingli@dlut.edu.cn Faculty of Management and Economics, Dalian University of Technology, No. 2 Linggong Road, Gangjingzi District, Dalian, Liaoning 116023, P.R. People's Republic of China

wrong hands in someday; then, the sensitive data could be copied or recovered by malicious people. Other similar insecure behaviours can be writing down passwords, delaying a backup, and sending unencrypted emails, etc. The shared characteristic of these behaviours is that the consequence caused by the behaviour is not immediate, but can be delayed, which could put an organisation's IS in a vulnerable state until negative outcomes occur sometime later. Such behaviour is a typical form of IS security policy violation, which we name it as consequence-delayed information security violation (CDISV).

CDISV has three particular characteristics: a. *The ultimate consequence caused by CDISV is delayed.* The ultimate outcome of CDISV does not unfold immediately, but at some time in the future. b. *CDISV is an indirect cause of IS damage.* Unlike other security violations, such as malicious destruction of information, running virus software, CDISV does not necessarily mean direct attack or other IS sabotage. Instead, the behaviour may provide opportunities for other people to further attack or destroy the IS, in this case, it could become the indirect cause of a security incident. c. *The risk created by CDISV could not be automatically eliminated.* During the period between CDISV happens and the ultimate consequence, the organisation's IS is in a vulnerable state, the risk will always exist until the behaviour is corrected. CDISV represents a significant threat to an organisation's IS, as it makes the IS vulnerable waiting for security incidents to happen, either attacked or exploited by insiders and outsiders. Due to the three characteristics mentioned above, employees easily overlook the seriousness of CDISV if they only focus on the immediate outcome of the behaviour rather than being aware of the possible delayed consequences in the future.

The above attributes of CDISV indicate a research gap in the existing literature. To our best knowledge, previous studies have not taken into account the temporal delay between an employee's CDISV and the consequences. There can be a difference in an employee's security-related behaviour decision based on the evaluation of immediate consequences and the decision based on the evaluation of future consequences. According to expected utility theory, people's decisions are based on both the probability and utility of future events (Kahneman and Tversky 1979; Schoemaker 1982). The more heavily people discount the future events the less certain they perceive it to be. In fact, people may perceive the immediate consequence of a risky behaviour as quite certain because they are immediately experienced, whereas they may perceive the future consequences as relatively uncertain because they are delayed. As the perceived uncertainty of delayed consequences increases, the previous approach such as threat appraisal in protection motivation theory (Boss et al. 2015; Johnston and Warkentin 2010) and benefit/cost analysis in rational choice theory (Bulgurcu, Cavusoglu, and Benbasat 2010) may lead people to decide to violate the security policy. Based on these approaches, people will perceive fewer risks and costs because of the perceived uncertainty of delayed consequences. However, we would like to argue that in addition to the risk assessment based approaches, from a temporal perspective that highlights employees' long-term, future-oriented beliefs and motivations in an organisation, we may find a way to prevent CDISV.

In this study, we want to understand employees' CDISV from a temporal perspective and examine two parts of their decision process. The first part concerns an individual's mindset he or she used to evaluate the possible delayed consequence in the current CDISV decision-making. The way that individuals establish this connection may enable them to make sense of their current behaviour, even when the future is not clear. This is especially important when people do not have enough information to predict the delayed outcomes of CDISV, but they are still expected to make security decisions. These connections help individuals answer questions such as whether or not it makes sense to consistently avoid CDISV when immediate harm is not caused every time, whether or not a current behaviour is helping to achieve an ultimate security goal, and whether or not it makes sense to sacrifice immediate convenience for future security. The common trend among these questions involves people making sense of their current behaviour by evaluating the possible future outcomes. We call this mindset long-term orientation (LTO) and it can influence employees' decisions on CDISV. The second part concerns employees' beliefs and needs generated in an organisation's context that can influence the formation of LTO and consequently affect their current behaviour decisions. According to the stewardship theory (Davis, Schoorman, and Donaldson 1997; Hernandez 2012), employees can see mutual benefits and risks within their organisation, and an individual's self-goals can be achieved through the success of the organisation. Since it usually takes time for an organisation to succeed, employees who identify with an organisation's values and focus on the higher-order needs (such as affiliation needs and growth needs) are more likely to develop LTO. In the context of CDISV, we argue that value identification and the fulfilments of particular higher-order needs can increase employees' LTO, which in turn may influence their CDISV. The findings of this study can help organisations design the IS security policies, security awareness training, as well as the security features in information systems.

The next section presents the theoretical background and the development of the hypotheses. We then present the data analysis and results. Finally, we discuss our findings, implications for research and practice, and limitations, and conclude our study.

## 2. Theoretical background and hypotheses development

Figure 1 shows the research model. The four core constructs proposed in our model are long-term orientation, value identification, trusted relationship fulfilment, and growth needs fulfilment. Since it is difficult and even illegal to monitor employees' CDISV in reality, we used intention of CDISV as a proxy, which is regarded to be highly correlated with behaviour (Ajzen 1988). We propose that employees' intention of CDISV is negatively influenced by LTO. Further, LTO is positively influenced by employees' value identification of avoiding CDISV, trusted relationship fulfilment, and growth needs fulfilment.

### *2.1. Long-term orientation*

In this study, LTO is conceptualised as an individual's mindset viewing the outcomes of CDISV over a long period of time. Mindset refers to people's general attitudes and the way they typically think about things (Sinclair 2003). It determines how an individual engages in events or views reality (Armstrong and Hardgrave 2007). LTO and similar concepts have appeared in the literature of psychology, marketing, management, etc., using terms such as 'managing for the long run' (Miller and Le Breton-Miller 2005), future orientation (Das and Teng 1997), consideration of future consequences (Strathman et al. 1994), conceptions of the future (Karniol and Ross 1996), and long-term orientation (Bearden, Money, and Nevins 2006; Hofstede 1991; Lumpkin, Brigham, and Moss 2010). Generally speaking, the literature has viewed LTO in several ways. Hofstede (1991) suggested LTO as a dimension of national values, which captures the extent to which a group of people have a future-oriented perspective rather than focusing on the present. Hofstede (1991) viewed LTO as a *cultural difference*; other literature has suggested that LTO may also be a variance in the form of organisation difference and individual difference. Lumpkin and Brigham (2011) defined LTO as 'the tendency to prioritise the long-range implications and impact of decisions and actions that come to fruition after an extended time period.' They described it as an organisation's *dominant logic*, which is 'a mindset or a worldview or conceptualisation of the business and the administrative tools to accomplish goals and make a decision in the business' (Prahalad and Bettis 1986). Bearden, Money, and Nevins (2006) defined LTO on an individual level as 'the cultural value of viewing time holistically, valuing both the past and the future rather than deeming actions important only for their effects in the here-and-now or the short term.' Das and Teng (1997) described a similar concept, future orientation, as 'individuals' psychological attributes regarding their perception of the future and the flow of time.' In agreement with the latter literature, our understanding of LTO in this study actually reflects an *individual difference* in regards to viewing the delayed consequence of CDISV.

Previous research has suggested that LTO has significant implications for people's choice of behaviour in an organisation. Studies have found that people with a LTO mindset within an organisation achieve better joint outcomes in integrative negotiations (Mannix, Tinsley, and Bazerman 1995) and are less likely to deplete organisational resources (Mannix 1991; Mannix and Loewenstein 1993). Employees who consider future consequences more are less likely to violate organisational rules (Takemura and Komatsu 2012). Employees with LTO often behave well beyond current legal requirements and avoid the compliance costs that come with stricter laws (Wang and Bansal 2012). Employees with a high degree of LTO and therefore have high consideration of future consequences are more likely to engage in prosocial behaviour (Joireman et al. 2006; Strathman et al. 1994) and be more safety-conscious (Graso and Probst 2012).

The theoretical basis for why an employee generates LTO is associated with a stewardship philosophy (Davis, Schoorman, and Donaldson 1997; Hernandez 2012; Le Breton-Miller and Miller 2011). Hernandez (2012) defined stewardship as 'the extent to which an individual willingly subjugates his or her personal interests to act in protection of others' long-term welfare.' The stewardship theory assumes that employees who hold a stewardship philosophy are collectivists, pro-organisational, and trustworthy rather than individualistic, opportunistic, and self-serving (Davis, Schoorman, and Donaldson 1997). This collectivism tendency is built upon the covenantal relationship between employees and their organisations. A covenantal relationship suggests that employees and organisations make a commitment to a shared set of values and a maximisation of the wellbeing of both the employee and the organisation (Joireman et al. 2006). It binds both the organisation and its employees to work toward a common goal without taking advantage of each other (Hernandez 2012). According to the theory, as long as employees want to share the benefits and risks together with an organisation, they are more likely to evaluate the consequences

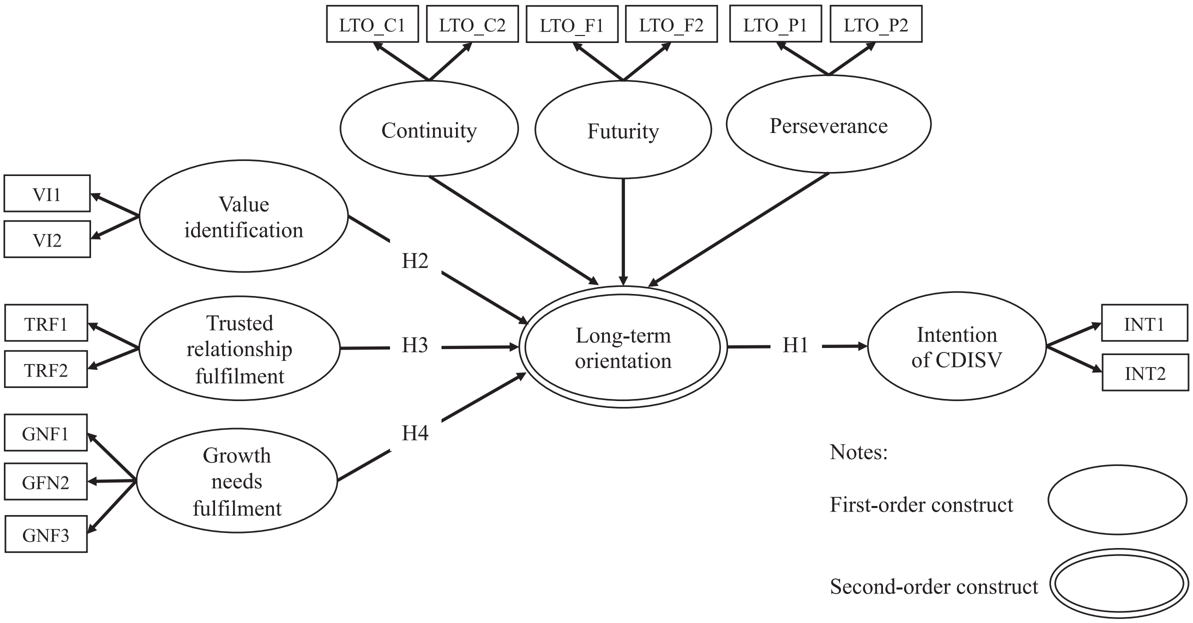

**Figure 1.** Research model.

of their behaviour with a long-term mindset, because any loss for the organisation means a loss for them in the end.

In the current study, the reason why employees choose to avoid CDISV could be the belief that they would share the benefit with their organisation if they avoid the delayed consequences of CDISV. If the organisation's interest is hurt, so do themselves in the end. For this reason, a LTO mindset could help them to make appropriate decisions for the current behaviour.

Drawing from Lumpkin and Brigham (2011), LTO is a multidimensional construct composed of three dimensions: (1) continuity, which addresses the necessity to keep doing a right thing; (2) futurity, which reflects a concern for future consequences; and (3) perseverance, which highlights how present decisions and actions affect the future. We discuss these three dimensions in more detail below.

*Continuity* is the belief that it is valuable to keep doing a right thing, consistently, without exception. In other words, people with continuity believe that what is right is worthy of preservation. Continuity emphasizes the present and future through repetition (such as making the same choice at 'all times' or 'every time') to convey the ongoingness and repetitiveness of actions. Hershfield, Cohen, and Thompson (2012) found that people who hold continuity beliefs are more likely to make ethical decisions. In the context of an organisation, employees' belief of continuity means an alignment between their ongoing decisions and the existing consensus made within the organisation, such as strategies and policies (Moss, Payne, and Moore 2014). In a context of IS security, it means employees respect the IS security policies and view compliance as the correct practice that should be preserved.

Regarding CDISV, an employee with a high degree of continuity may believe that avoiding CDISV at work has value; therefore, persisting with such behaviour is still valuable in the future as it is now. Such persistence would cause the employee to avoid CDISV every time he or she confronts risky situations.

*Futurity* is the belief that the process of forecasting, planning, and evaluating the long-range consequences of current actions has utility (Lumpkin and Brigham 2011). Individuals with futurity pay more attention to, care more about, and give greater weight to the possible future outcomes of their current behaviour when making decisions about how to behave (Joireman et al. 2006). Zimbardo, Keough, and Boyd's (1997) five-factor model may be used to identify an individual's future orientation. Zimbardo and colleagues suggested that individuals with future orientation actively plan for and strive to meet future goals. They see themselves as achievers, tend to be conscientiousness and have a preference for consistency. Individuals with futurity generally avoid sensation seeking, aggression, impulsivity, and risk-taking because such behaviours are antithetical to future success (Zimbardo, Keough, and Boyd 1997). Previous empirical studies have also shown that decision-makers who have a high degree of futurity make less risky decisions (Das and Teng 1997).

In the context of CDISV, an employee with a high degree of futurity may take both current and future consequences of behaviour into consideration. For example, when an employee thinks about using a personal unencrypted USB drive to store confidential corporate data, he or she may consider whether or not the data could be leaked if the drive fell into the wrong hands in the future. Since employees with a high degree of futurity value the future impact of current behaviour, the undesired future outcomes may prevent the CDISV.

*Perseverance* is the belief that efforts made today will pay off in the future (Lumpkin and Brigham 2011). People with perseverance are typically willing to sacrifice immediate benefits in order to get long-term benefits. These individuals believe that certain behaviours are worthwhile because of future benefits, even though immediate outcomes are relatively undesirable or require immediate costs. They are willing to sacrifice immediate benefits like pleasure or convenience in order to achieve more desirable future states (Strathman et al. 1994). Bearden, Money, and Nevins's (2006) study of LTO used items such as 'I don't mind giving up today's fun for success in the future' that were suggestive of perseverance. The trade-offs between short-term costs and long-term benefits have been discussed in the context of organisations extensively. Researchers have considered organisational citizenship behaviour to be a social dilemma (Joireman et al. 2006) in which short-term individual and long-term collective interests are at odds (Komorita and Parks 1994). Joireman et al. (2006) found that employees who place greater value on future outcomes than immediate outcomes are more likely to engage in organisational citizenship behaviour.

In the context of CDISV, an employee with a high degree of perseverance may believe that it is worth sacrificing immediate fun or convenience if such behaviour can ensure IS security in the future. However, most employees are not rewarded for complying with security policy (Vroom and von Solms 2004). In fact, complying with IS security policies can be time-consuming or burdensome and may require additional efforts (Bulgurcu, Cavusoglu, and Benbasat 2010; Vroom and von Solms 2004; Warkentin, Davis, and Bekkering 2004). Since CDISV may be highly embedded into work (e.g. using an unencrypted USB device), it may seem costly to keep avoiding such behaviours in the absence of a formal reward (Straub and Welke 1998). However, if employees have the belief of perseverance, they may value the effectiveness of their actions, believe that the efforts made today will be paid back in the future, and therefore overcome the current inconvenience. As a result, employees with such beliefs may have more chances to sacrifice immediate benefits to keep avoiding CDISV in order to contribute to a long-term safety environment.

Together, employees' LTO (formed by continuity, futurity, and perseverance) may negatively influence their intention of CDISV. Thus, we generated our first hypothesis:

> H1: The degree of an employee's LTO is negatively associated with the employee's intention of CDISV.

### 2.2. Antecedents of LTO

Since LTO plays an important role in decreasing an employee's CDISV, it is worthy of discussing what factors facilitate employees to create a LTO. Scholars have proposed that higher order needs, intrinsic factors, and identification are important in motivating individuals to become stewards of the organisation (Davis, Schoorman, and Donaldson 1997; Hernandez 2012). The fulfilment of the higher order needs can be seen as intrinsic rewards for steward-like employees. These rewards include opportunities for growth, achievement, affiliation, and self-actualisation (Davis, Schoorman, and Donaldson 1997), which can be found in need theories (Alderfer 1972; Maslow et al. 1970; McClelland 1975). These rewards are similar in that they are time-consuming and difficult to obtain through the individual's own power. Since a steward-like employee's interests and the organisation's interests are consistent, such an individual's needs can be satisfied via the organisation's achievements over a relatively long period. Davis, Schoorman, and Donaldson (1997) also recognised that identification with and commitment to the organisation can facilitate an individual's motivation to promote the success of the organisation (Hernandez 2012). In CDISV context, we will argue that an employee's LTO is associated with two types of psychological factors: value identification and the fulfilment of higher-order needs.

#### 2.2.1. Value identification

Identification refers to the belief in and acceptance of an organisation's mission, vision, and objectives (Mael and Ashforth 1992). Identification is an important psychological profile of a steward-like employee who holds a LTO mindset. An employee with a high degree of identification will believe it makes sense to work toward an organisation's goals, solve problems, and overcome barriers that prevent the consistent, successful completion of tasks and assignments (Davis, Schoorman, and Donaldson 1997). A strong identification with and belief in an organisation's goals enhance the employee's willingness to exert considerable efforts on behalf of the organisation in order to achieve a shared goal in the future (Mowday, Porter, and Steers 2013; O'Reilly and Chatman 1986). In general, researchers have agreed that identification leads to employees believing that helping organisations accomplish their objectives in the long run is important (Besharov 2014). When employees have a high identification with the organisational goals, they are more likely to be long-term oriented because they understand that achieving goals usually requires time.

There could be various types of identification regarding an organisation's value, mission, or vision. We specifically define *value identification (*VI) in the context of CDISV as the extent to which employees identify with the meaning and value of the IS security that an organisation preaches. As we have already indicated, due to the fact that there could be a delay between the behaviour and the consequence, it usually takes time and effort to evaluate the effectiveness of IS security measures and the outcome of employees' behaviours. Employees who recognise and accept the underlying value of the security behaviour may think it is necessary to avoid CDISV consistently, even when the information about the delayed consequence is not clear. We propose that value identification will make employees recognise the necessity of considering the long-term consequences of CDISV. Thus, we generated a second hypothesis:

> H2: An employee's value identification of the meaning and value of IS security is positively associated with the employee's LTO with respect to CDISV.

### 2.2.2. Fulfilment of higher-order needs

As the stewardship theory suggests, the fulfilment of higher-order needs as intrinsic motivations is important in generating LTO (Davis, Schoorman, and Donaldson 1997; Hernandez 2012). Examples of higher-order needs are esteem, achievement, opportunities for growth, affiliation, self-actualisation, etc., which can be found in need theories (e.g. Alderfer 1972; Maslow et al. 1970). The fulfilment of higher-order needs is seen to be an intrinsic reward for steward-like employees (Davis, Schoorman, and Donaldson 1997). These rewards are similar in that they are time-consuming and difficult to obtain through the individual's own power. Since a steward-like employee's interests and an organisation's interests are consistent, such an individual's needs can be satisfied via the organisation's achievements over a relatively long period. Therefore, employees could generate LTO regarding a specific behaviour by the satisfaction of such higher-order needs via that behaviour.

In the context of our research, we propose that two types of higher-order needs are relevant to CDISV: the need for a trusted relationship and the need for growth. *Trusted relationship fulfilment* (TRF) refers to an employee's perception of the extent to which avoiding CDISV fulfils his or her need for developing a trusted relationship. A trusted relationship is a higher-order need that a steward-like employee pursues in an organisational environment (Davis, Schoorman, and Donaldson 1997). Maintaining relationships is a dynamic process. People must continually invest time and effort to maintain an established relationship. Therefore, if an individual perceives that behaviour can help him or her to enhance a relationship, he or she may think it is worth engaging in such behaviour consistently. Regarding CDISV, avoiding CDISV at work can help an employee to establish a trusted relationship, for the behaviour usually protects the confidentiality and integrity of work data and therefore protects the work of other colleagues. Employees who rarely engage in CDISV may be regarded as responsible and trusted co-workers (Flowerday and von Solms 2005). However, the trusted relationship requires time to establish and maintain. As a result, individuals who perceive the benefits of avoiding CDISV in terms of trusted relationship development may generate a LTO and believe that continuing to avoid CDISV is meaningful. In this case, they take into consideration the long-term influence of CDISV on the maintenance of the trusted relationship. Thus, we generated a third hypothesis:

> H3: An employee's trusted relationship fulfilment is positively associated with the employee's LTO.

*Growth needs fulfilment* (GNF) refers to an employee's perception of the extent to which avoiding CDISV is able to fulfil his or her need for growth. In the current context, *growth* typically refers to the knowledge of IS security and the ability to deal with security-related situations. IS develops very quickly. Learning to use new technology and solve problems in a new system can give people the feeling of achievement and therefore increase an individual's willingness to keep using the system (Au, Ngai, and Cheng 2008). The feeling of self-growth arises when people confront what they view as an optimal challenge (Deci and Flaste 1995). These findings about higher-order needs and performance are consistent with the assumptions of the stewardship theory, which notes that an employee's personal needs are met by working toward organisational, collective ends (Davis, Schoorman, and Donaldson 1997). In the context of CDISV, employees who have growth needs are willing to master security-related knowledge and are able to deal with different risky situations and solve security problems, which offers employees opportunities to demonstrate their capabilities at work. For example, in order to avoid downloading suspicious files from the Internet, employees should instead be able to find more secure sources. The feeling of personal achievement can be seen as an intrinsic reward. In order to practice this capability, employees may be willing to think more about the possible consequences of CDISV, including consequences in the future, which may generate LTO. Thus, we generated a fourth and final hypothesis:

H4: An employee's growth needs fulfilment is positively associated with the employee's LTO.

### 2.3. Control variables

Our model includes eight control variables: gender, age, type of contract, years of working in the company, years of computer use, information technology (IT) knowledge, and two dummy variables for controlling the effects of three violation scenarios. Previous literature has confirmed that younger people and males are more likely to engage in illicit behaviour (Leonard and Cronan 2005; Pratt et al. 2006). IS literature has also suggested that computer experience is negatively related to technology misuse (Loch and Conger 1996). We further predict that a lack of IT knowledge may be a reason for CDISV and may relate to an individual's needs for growth. Years of working in the company and the type of contract may be relevant to an employee's stewardship behaviour. Research has indicated that longer employment may promote LTO (Miller and Shamsie 2001; Zahra 2005).

## 3. Methodology

IS security research has used three methods for measuring the dependent variable: generic measures, specific measures without the context, and specific measures with the context (Siponen and Vance 2014). Of these three methods, we selected specific measures with the context, or scenarios, to measure the dependent variable for two reasons. The first reason was that it provides more details and contextual specificities (Nagin and Paternoster 1993). This is important because information security actions can be context specific; for example, depending on the work the employees do, the common CDISV in each environment may be different. We collected data from a large organisation operating in different countries with different departments. If we used generic measures such as 'I use insecure USB practices,' people may have different interpretations toward the behaviour due to the lack of specific conditions. The use of scenarios allowed us to provide the same and sufficient information for all employees regarding the noncompliance. The second reason for selecting the scenario method was its nonintrusive way of responding to sensitive issues (Nangin and Pogarsky 2001).

### 3.1. Scenario design

In order to make realistic and believable scenarios, we designed the scenarios together with the security managers of the company where we collected the data. First, the security managers listed the IS security problems that concerned them, covering a wide range of issues such as the secure use of mobile devices, secure emailing, secure behaviour when travelling, and secure use of the Internet. Based on their list, we composed specific scenarios. The security managers then evaluated whether or not these scenarios were relevant to their situations, and they helped edit them. After two rounds of modifications, we finalised three scenarios that were regarded as the most relevant to the company: unauthorised portable devices for storing corporate data, sending unencrypted emails, and downloading suspicious files from the Internet. The specific scenarios are shown in Appendix A.

### 3.2. Instruments

Guided by Siponen and Vance (2014), who suggested measuring specific examples of IS security policy violations to get more accurate measures, we used specific scenarios as described above. In addition, we measured both the dependent variable and the independent variables in specific ways. For example, to measure intention, we asked, 'If you were Newman, what is the likelihood that you would have copied the file onto a personal unencrypted USB stick?' To measure continuity, we asked respondents to evaluate statements such as, 'It is valuable that I always avoid the behaviour without exception.' In the survey, we explained that 'the behaviour' referred to Newman's action as described in the scenario (e.g. copying the file onto a personal unencrypted USB stick). We measured the dependent variable, intention of CDISV, using two items adapted from D'Arcy, Hovav, and Galletta (2009).

We treated LTO as a formative construct. Conceptually, the three dimensions (continuity, futurity, and perseverance) share similarities to the extent that they describe a single construct (LTO), but they also each explain a different facet of the LTO construct (Brigham et al. 2014). Therefore, we formatively constructed LTO by three reflective first-order constructs (e.g. continuity, futurity, perseverance). We measured continuity (LTO_C), futurity (LTO_F), and perseverance (LTO_P) using two items adapted from Brigham et al. (2014). We measured value identification (VI) using two items adapted from Davis, Schoorman, and Donaldson (1997). We measured trusted relationship fulfilment (TRF) using two items adapted from Deci et al. (1991). We adapted the three items that measured growth needs fulfilment (GNF) from Alderfer (1972). We assessed the measures for dependent and independent variables using a 7-point Likert scale. Aside from the scale of intention of CDISV (INT1) that was anchored from 1 (very unlikely) to 7 (very likely), the rest of the item scales were anchored from 1 (strongly disagree) to 7 (strongly agree). For the control variable of gender, male was coded as 1 and female was coded as 2. Age was categorised into 1 (18–25), 2 (26–35), 3(36–45), 4 (46–55), 5(56–65), and 6(66 and above). For the type of work contract, a fixed term contract was coded as 1, and a permanent term contract was coded as 2. We measured IT knowledge using a 7-point Likert scale ranging from 1 (very low) to 7 (very high). The region of the country was categorised into 1 (Canada), 2 (Hong Kong), 3 (Singapore), 4 (South Africa), 5 (United Kingdom), and 6 (United States). We measured both the time working in the company and the time of computer use in years. We used two dummy variables to represent the three categorical scenarios (Sumo et al. 2016; Vinzi et al. 2010). They were coded as follows: Scenario 1 (DummyS1=1, otherwise = 0), Scenario 2 (DummyS2=1, otherwise = 0). Scenario 3 (Both DummyS1 and DummyS2 were coded as 0). The full instrument is provided in Appendix B.

### 3.3. Pilot study

We conducted a pilot study before the primary data collection. Since the wordings were just slightly different among the three scenarios, we used one scenario (unauthorised portable devices for storing corporate data) to pilot the survey. We invited our faculty members, PhD students, and any researchers familiar with the topic to complete the survey and provide comments on our questions. The pilot sample size was 39. We assessed reliability by using Cronbach's α, and the convergent and discriminant validity by using principal components analysis. The assessment indicated acceptable results for the instrument.

### 3.4. Sample and data collection

We conducted the primary data collection at a global insurance company that owns offices in more than 70 countries, has more than 3,500 employees, and serves more than 160 countries. The security manager suggested that we randomly send the survey to 670 employees in the following six countries: Canada, Hong Kong, Singapore, South Africa, the United Kingdom, and the United States. We composed the survey in English and made it available online. We sent an email to each selected employee that contained the consent statement as well as the survey link. In order to maximally respect employees' rights, the statement informed that employees were invited to voluntarily participate in the survey to help improve the organisation's IT environment; their answers were kept anonymous and only for research purpose; some demographic information was requested only needs to be answered if they are willing to. Employees were free to choose whether answering the survey or not. They will not be identified in any ways through their answers. We randomly assigned each respondent to one of the three scenarios and corresponding questions. The duration of the data collection was 18 days. We received 170 responses, a response rate of 25.4%, after a single reminder on the 10 th day. The demographic information is shown in Table 1.

To test the nonresponse bias, we followed the post-hoc strategy for estimating nonresponse errors as proposed by Sivo et al. (2006). We compared the early one-third of the respondents ($N = 56$) to the last one-third of the respondents ($N = 56$) for all answers. All $t$-test comparisons between the means of the early and late responses showed no significant differences, which indicates the nonresponse bias is not a problem in this study.

## 4. Data analysis and results

We tested the proposed model empirically by using the partial least square-based structural equation modelling (PLS-SEM) technique, with the statistical software package SmartPLS v3 .2 .7 (Ringle, Wende, and Becker 2015).

**Table 1.** Demographic information.

| Demographics | Frequency | Percentage |
|---|---|---|
| Gender | | |
| Male | 89 | 52.4% |
| Female | 81 | 47.6% |
| Age | | |
| 18–25 | 4 | 2.4% |
| 26–35 | 34 | 20.0% |
| 36–45 | 45 | 26.5% |
| 46–55 | 53 | 31.2% |
| 56–65 | 31 | 18.2% |
| 66 and above | 3 | 1.8% |
| Type of work contract | | |
| Fixed term | 35 | 20.6% |
| Permanent term | 135 | 79.4% |
| IT knowledge | | |
| 1 (Very low) | 4 | 2.4% |
| 2 | 13 | 7.6% |
| 3 | 24 | 14.1% |
| 4 | 54 | 31.8% |
| 5 | 44 | 25.9% |
| 6 | 18 | 10.6% |
| 7 (Very high) | 13 | 7.6% |
| Country of origin | | |
| Canada | 8 | 4.7% |
| Hong Kong | 10 | 5.9% |
| Singapore | 15 | 8.8% |
| South Africa | 3 | 1.8% |
| United Kingdom | 34 | 20.0% |
| United States | 100 | 58.8% |
| Participants in each scenario | | |
| Scenario 1 | 56 | 32.9% |
| Scenario 2 | 50 | 29.4% |
| Scenario 3 | 64 | 37.6% |

Note: N = 170.

The reasons for using PLS in this study are, first, our model includes a formative construct (i.e. LTO) and PLS is particularly well suited to estimate this type of model (Hair et al. 2017). Second, variance-based SEM techniques provide better results than covariance-based SEM techniques when estimating complex models with higher-order constructs (e.g. LTO) (Becker et al. 2012). Third, PLS-SEM has less restricts on sample distributions and sample size.

### 4.1. Evaluation of model fit

Henseler, Hubona, and Ray (2016) recommend the evaluation of global model fit as the preliminary step of PLS model assessment. They suggest examining the following model fit indexes: (1) the standardised root mean squared residual (SRMR); (2) the unweighted least squares discrepancy ($d_{\mathrm{ULS}}$); and (3) the geodesic discrepancy ($d_{\mathrm{G}}$). The SRMR is defined as the difference between the observed correlation and the model implied correlation matrix. Henseler et al. (2013) introduced the SRMR as a goodness of fit measure for PLS-SEM, which can be used to avoid model misspecification. A value less than 0.08 (Hu and Bentler 1998) is considered a good fit. The $d_{\mathrm{ULS}}$ and $d_{\mathrm{G}}$ are the measures that quantify how strongly the empirical correlation matrix differs from the model-implied correlation matrix. The lower the $d_{\mathrm{ULS}}$ and $d_{\mathrm{G},}$ the better the theoretical model's fit (Dijkstra and Henseler 2015). The confidence interval should include the original value. Hence, the upper bound of the confidence interval should be larger than the original value of the fit criteria to indicate that the model has a good fit. Our results in Table 2 revealed that the SRMR value is 0.046 that is below the threshold of 0.08 for acceptable fit in PLS-SEM. The tests of model fit indexes are all below the upper bound of the confidence interval at 99% percentiles (HI99).[1] This implies that this model cannot be rejected (Henseler, Hubona, and Ray 2016).

### 4.2. Assessment of the measurement model

For the reflective constructs, we assessed internal consistency and convergent validity by examining item loading, Cronbach's α, composite reliability, and average variance extracted (AVE) (Gefen and Straub 2005). We compared the results (Table 3) with the commonly accepted guidelines. For reliability, the composite reliability of the constructs was greater than 0.8 (Nunnally 1978), and Cronbach's α was greater than 0.7 (Chin 1998). For convergent validity, indicator loadings exceeded 0.7 (Chin 1998), and AVE for each reflective construct exceeded 0.5. We performed a bootstrap with 1,000 resamples and examined the *t*-values of the outer model loadings. All the indicators exhibited loadings that were significant ($p < 0.001$), denoting strong convergent validity.

**Table 2.** Model fit.

| | Value | HI95 | HI99 |
|---|---|---|---|
| SRMR | 0.046 | 0.043 | 0.047 |
| $d_{\mathrm{ULS}}$ | 0.449 | 0.379 | 0.468 |
| $d_{\mathrm{G1}}$ | 0.517 | 0.840 | 0.980 |
| $d_{\mathrm{G2}}$ | 0.364 | 0.399 | 0.495 |

For the discriminant validity, all items loaded higher on their respective constructs than on the other constructs, and the cross-loading differences were much higher than the suggested threshold of 0.1 (Gefen and Straub 2005; Table 4). The square root of the AVE of each construct was higher than the inter-construct correlations (Fornell and Larcker 1981; Table 5). The correlations among all constructs were all well below the 0.90 thresholds, suggesting that all constructs were distinct from each other (Herath and Rao 2009).

In the model, LTO is a second-order construct. It is a reflective-formative type of hierarchical component model. LTO is formatively constructed by three reflective first-order constructs (i.e. continuity, futurity, perseverance). We followed the two-stage approach suggested by Ringle, Sarstedt, and Straub (2012) to test the hierarchical component model. First, we used the repeated indicators approach to obtain the latent variable score for the lower order components. Second, we used the latent variable scores as manifest formative indicators of the second-order construct (Wetzels, Odekerken-Schröder, and van Oppen 2009).

We validated our formative construct—LTO, separately from the reflective constructs. The weights of indicators contributing to LTO were all significant, which denotes good validity. Additionally, we examined the variance inflation factor (VIF) statistic for the three indicators. The VIF score was no more than 1.9, well below the 3.3 thresholds (Petter, Straub, and Rai 2007), which means that multicollinearity does not exist in the model and that the model has good reliability. Based on these tests results, we conclude that LTO has sufficient construct validity and reliability.

Our validation results suggest that all reflective measures demonstrated satisfactory reliability and construct validity and that the formative measures demonstrated satisfactory construct validity and no significant multicollinearity. Therefore, all of the measures were valid and reliable.

### 4.3. Common method variance

We also assessed the common method variance (CMV). Because we collected the data from a single source (i.e. an

**Table 3.** Reliability and convergent validity for reflective constructs.

| Construct | Sub-construct | Indicator | Loading | t-statistic | Residual | Cronbach's α | Composite reliability | AVE |
|---|---|---|---|---|---|---|---|---|
| INT | N/A | INT1 | 0.93 | 47.61*** | 0.14 | 0.85 | 0.93 | 0.87 |
| | | INT2 | 0.94 | 55.92*** | 0.12 | | | |
| LTO | LTO_C | LTO_C1 | 0.95 | 84.90*** | 0.10 | 0.90 | 0.95 | 0.91 |
| | | LTO_C2 | 0.96 | 127.44*** | 0.09 | | | |
| | LTO_F | LTO_F1 | 0.90 | 32.13*** | 0.20 | 0.77 | 0.90 | 0.81 |
| | | LTO_F2 | 0.91 | 27.50*** | 0.18 | | | |
| | LTO_P | LTO_P1 | 0.93 | 45.23*** | 0.14 | 0.84 | 0.93 | 0.86 |
| | | LTO_P2 | 0.93 | 60.57*** | 0.14 | | | |
| VI | N/A | VI1 | 0.94 | 79.23*** | 0.11 | 0.88 | 0.94 | 0.89 |
| | | VI2 | 0.94 | 88.88*** | 0.11 | | | |
| TRF | N/A | TRF1 | 0.95 | 55.42*** | 0.09 | 0.91 | 0.96 | 0.92 |
| | | TRF2 | 0.96 | 88.36*** | 0.08 | | | |
| GNF | N/A | GNF1 | 0.92 | 59.21*** | 0.15 | 0.83 | 0.90 | 0.75 |
| | | GNF2 | 0.83 | 17.63*** | 0.32 | | | |
| | | GNF3 | 0.84 | 19.52*** | 0.30 | | | |

individual employee) at a single point in time, CMV could unduly sway the results (Podsakoff et al. 2003). We attempted to mitigate this bias by adopting multiple techniques. Specifically, we used both procedural remedies and statistical remedies.

As for the procedural remedies, we first conducted pilot studies for the questionnaire to eliminate ambiguous items. Second, we informed the participants that their responses would be confidential and assured them that there were no right or wrong answers. Third, we used a nonintrusive method of technical scenarios to let the participants imagine the situation described before making their decisions rather than ask them about their own behaviour directly. Finally, we randomly sorted the question order to reduce hypothesis guessing.

As for statistical remedies, since each method used by previous studies had advantages and disadvantages (Chin, Thatcher, and Wright 2012), we used several methods to identify the problem collectively. First, we conducted Harman's one-factor test by including all items in a principal components factor analysis (Podsakoff et al. 2003). Evidence for CMV exists when one factor accounts for most of the covariance. The results revealed four factors with no single factor accounting for a majority (<50%) of variance, suggesting no substantial CMV among the scales. Second, we used a partial correlation method (Lindell and Whitney 2001; Podsakoff et al. 2003). Given that we did not include any constructs that were completely theoretically unrelated to one or more constructs in our model, we followed Pavlou, Liang, and Xue (2007) and used a construct that was weakly related to other constructs as the marker variable. We used its average correlation with the principal study variables ($r = 0.026$) as the CMV estimate. Following Malhotra, Kim, and Patil (2006), we developed a CMV-adjusted correlation matrix and examined the CMV-adjusted structural relationships in our research model.[2] We found no changes in significance after accounting for the distinct construct, suggesting the effect of CMV was minimal. Finally, we followed Lindell and Whitney (2001), Malhotra, Kim, and Patil (2006), Richardson, Simmering, and Sturman (2009), and Williams, Hartman, and Cavazotte (2010) to conduct a confirmatory factor analysis (CFA) marker test in AMOS 22. Specifically, to assess method variance, we specified a hypothesised method factor as an underlying driver of all of the indicators in the measurement model. The fit indices of the model including the method factor

**Table 4.** Loadings and cross-loadings.

| Construct | Sub-construct | Indicator | INT | LTO_C | LTO_F | LTO_P | VI | TRF | GNF |
|---|---|---|---|---|---|---|---|---|---|
| INT | N/A | INT1 | **0.93** | −0.56 | −0.29 | −0.45 | −0.47 | −0.40 | −0.39 |
| | | INT2 | **0.94** | −0.58 | −0.38 | −0.47 | −0.54 | −0.50 | −0.31 |
| LTO | LTO_C | LTO_C1 | −0.57 | **0.95** | 0.53 | 0.54 | 0.75 | 0.53 | 0.54 |
| | | LTO_C2 | −0.59 | **0.96** | 0.64 | 0.62 | 0.78 | 0.59 | 0.57 |
| | LTO_F | LTO_F1 | −0.30 | 0.48 | **0.90** | 0.61 | 0.54 | 0.47 | 0.37 |
| | | LTO_F2 | −0.36 | 0.63 | **0.91** | 0.52 | 0.71 | 0.46 | 0.44 |
| | LTO_P | LTO_P1 | −0.44 | 0.56 | 0.61 | **0.93** | 0.55 | 0.55 | 0.35 |
| | | LTO_P2 | −0.47 | 0.58 | 0.56 | **0.93** | 0.51 | 0.58 | 0.39 |
| VI | N/A | VI1 | −0.50 | 0.77 | 0.64 | 0.50 | **0.94** | 0.54 | 0.47 |
| | | VI2 | −0.52 | 0.75 | 0.67 | 0.57 | **0.94** | 0.60 | 0.51 |
| TRF | N/A | TRF1 | −0.45 | 0.54 | 0.47 | 0.56 | 0.55 | **0.95** | 0.49 |
| | | TRF2 | −0.47 | 0.59 | 0.52 | 0.61 | 0.60 | **0.96** | 0.52 |
| GNF | N/A | GNF1 | −0.36 | 0.60 | 0.42 | 0.37 | 0.55 | 0.49 | **0.92** |
| | | GNF2 | −0.28 | 0.42 | 0.38 | 0.35 | 0.39 | 0.43 | **0.83** |
| | | GNF3 | −0.32 | 0.48 | 0.36 | 0.31 | 0.39 | 0.44 | **0.84** |

**Table 5.** Latent variable correlations and the square root of AVE.

| Construct | Mean | Standard deviation | INT | LTO | VI | TRF | GNF |
|---|---|---|---|---|---|---|---|
| INT | 2.65 | 1.89 | **0.92** | | | | |
| LTO | 5.76 | 1.25 | −0.61 | – | | | |
| VI | 5.83 | 1.06 | −0.54 | 0.83 | **0.94** | | |
| TRF | 5.06 | 1.23 | −0.48 | 0.64 | 0.60 | **0.96** | |
| GNF | 5.39 | 1.21 | −0.38 | 0.59 | 0.52 | 0.53 | **0.87** |

Note: Bold items are the square root of the AVEs.

were not significantly better than the original one ($\chi^2 = 24.976$, df = 15, $p = 0.0503$). All the results mentioned above collectively suggest that the CMV was not serious in our study.

### 4.4. Theoretical model test

#### 4.4.1. The main effects model

Our PLS results of the full model were consistent with our theory, as shown in Figure 2. LTO had a significant negative effect (path coefficient = −0.58, $p < 0.001$) on intention of CDISV, which supports H1. VI had a significant positive effect (path coefficient = 0.64, $p < 0.001$) on LTO, which supports H2. TRF had a significant positive effect (path coefficient = 0.17, $p < 0.05$) on LTO, which supports H3. GNF had a significant positive effect (path coefficient = 0.17, $p < 0.05$) on LTO, which supports H4.

LTO explained 43% of the variance in the intention of CDISV. VI, TRF, and GNF collectively explained 74% of the variance in LTO. For the control variables, contract type and two dummy variables representing the three scenarios are significant. In summary, the results provide support for all of the hypotheses we proposed.

#### 4.4.2. The mediation effect

We also tested the possible mediation effect in the model. This study follows the guidelines for testing mediation effects in PLS-SEM (Nitzl, Roldan, and Cepeda 2016; Preacher and Hayes 2008, Zhao, Lynch, and Chen 2010). The method suggests that, first, using a bootstrap procedure to test the significance of indirect effect from the independent variable to the dependent variable via the mediator. If the indirect effect is significant, there exists a mediation effect. Second, determine the type of mediation. If the indirect effect is significant whereas the direct effect is not significant, it means it is a full mediation. By contrast, if the direct effect is significant, then it is a partial mediation. The mediation test is implemented in SmartPLS 3.2.7 (Hair et al. 2017). Table 6 lists the testing results. The results show that LTO partially mediates the relationship between VI and INT, and the relationship between TRF to INT. The indirect effect from GNF to INT nearly reaches a significant level ($p = 0.07$), and the respective direct effect is not significant, indicating a marginally significant full mediation.

## 5. Discussion

### 5.1. Main findings

The empirical results supported all our hypotheses. We found that LTO significantly decreases employees' CDISV intention (H1 was supported). This finding is consistent with previous studies suggesting that LTO decreases an individual's risk-taking behaviours, including entrepreneurs' risk decisions (Das and Teng 1997), risky life behaviours such as smoking or using drugs (Keough, Zimbardo, and Boyd 1999), and employees' rule violation in organisations (Takemura and Komatsu 2012). Specifically, our results suggest that employees who hold the three long-term related beliefs in mind are less likely to engage in CDISV, as they (1) respect the value of consistent good security practices, (2) take future consequences of current behaviour into account, and (3) are willing to sacrifice immediate benefit to achieve long-term security goals. Although the three dimensions represent different facets of the LTO, the results reveal that the strength of each dimension is not equal in our CDISV context. The weight of continuity (weight = 0.76) is higher than that of futurity (weight = 0.16) and perseverance (weight = 0.18), indicating that an employee's belief of whether one should always comply with the security policy without exception represents a main form of LTO. An explanation for the weight variation could be that futurity and perseverance may require employees to evaluate the potential negative influence on organisations due to their violation and whether the outcome is worth their efforts. Such evaluations may require further security-related experience or knowledge. While, continuity is a more simple belief in terms of whether a behaviour is allowed or not in policy, which is easy to generate. Another reason is that continuity may be already a mature belief for our sample participants thanks to the organisation's security training, however, the current training may lack of the content focusing on the other two facets of LTO, futurity and perseverance, which needs improvement in the future training design.

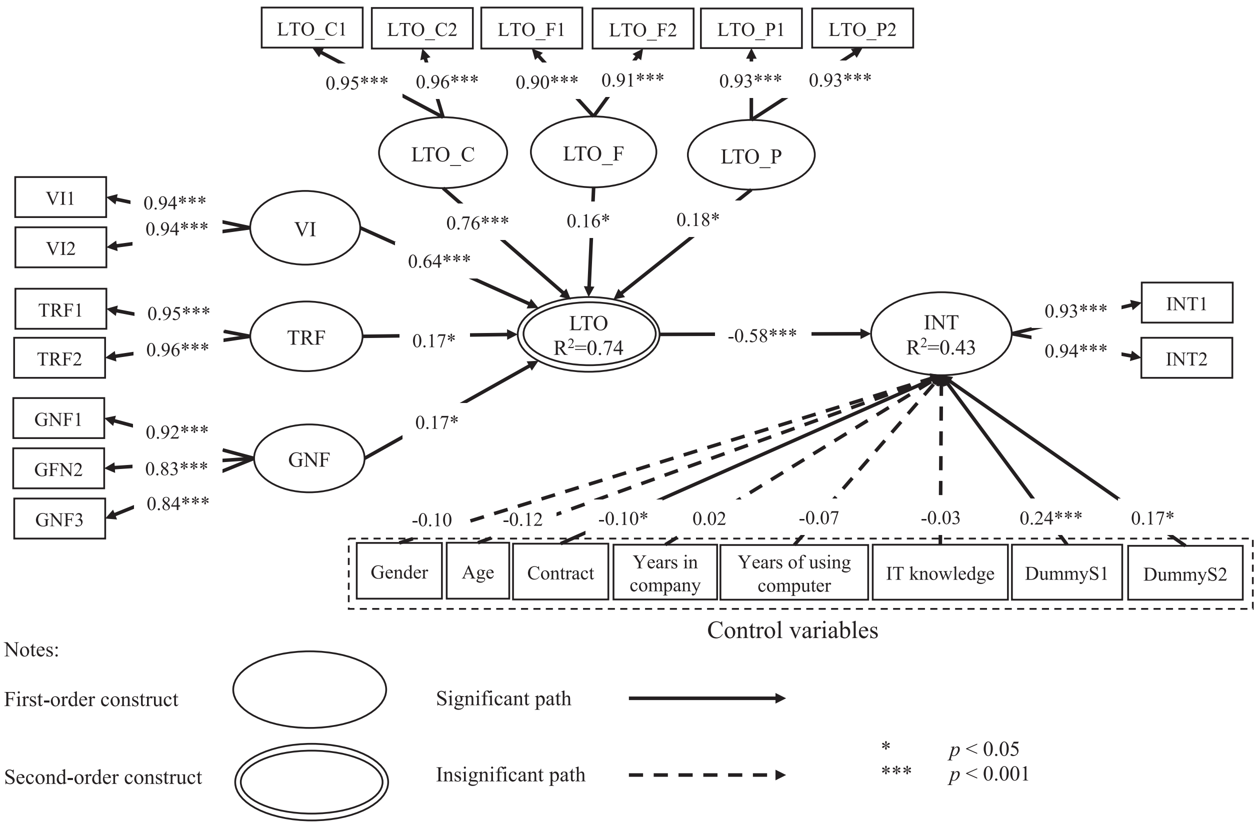

**Figure 2.** Structural model results.

In terms of the antecedents of LTO, all the three factors were confirmed to positively influence LTO. Specifically, we found that the more employees identify with organisational IS security goals and policies, the more likely they are to generate a LTO toward CDISV-avoiding activities (H2 was supported). This result indicates that employees with value identification will not only consider the on-going behaviour outcomes but will also pay attention to the future consequences of their acts, which is a reflection of a deep understanding of and strong agreement with organisational IS security policies. In IS research, Bateman, Gray, and Butler (2011) got similar findings that when the members of a virtual community recognise the value of the community, they will persist in staying in the community.

We also found that the fulfilment of two types of employee needs (the need for trusted relationships and the need for growth) significantly influenced the emergence of an employee's LTO (H3 and H4 were supported). These findings indicate that, although avoiding CDISV may require more effort on the employees' part, they will think that avoiding CDISV consistently is meaningful (1) if they feel that such behaviour will help them be recognised as trustworthy and reliable workers in the organisation and/or (2) if it challenges their abilities to deal with risky situations. More importantly, our findings confirm that the two types of needs require time to fulfil, therefore leading to LTO.

In addition, regarding the strength of the three factors, our results revealed that value identification has a bigger impact (path coefficient = 0.64, $p < 0.001$) than that of trusted relationship fulfilment (path coefficient = 0.17, $p < 0.05$) and growth needs fulfilment (path coefficient = 0.17, $p < 0.05$). This indicates that identifying with the security policies is much more important in generating a LTO than fulfilling the two higher-order needs in our context. The former is the perception about the organisation, whereas the latter two are the perceptions about self. According to stewardship theory, a steward-like employee view organisation's interests

**Table 6.** Results of mediation test.

| Path | Specific indirect effects | Direct effect | Total effect | Types of mediation |
|---|---|---|---|---|
| VI to INT via LTO | −0.30*** ($p < 0.001$) | −0.34*** | −0.34*** | Partial |
| TRF to INT via LTO | −0.08* ($p < 0.05$) | −0.22* | −0.22* | Partial |
| GNF to INT via LTO | −0.08 ($p = 0.07$) | −0.06 | −0.06 | Full (marginal) |

ahead of personal self-interests (Hernandez 2012). In this sense, our results have confirmed stewardship theory in a security management context.

Our further mediation test has confirmed the mediation role of LTO. We found that LTO fully mediates the effect of growth needs fulfilment on CDISV. And, the effects of value identification and trusted relationship fulfilment are partially mediated, indicating that they have direct effects on intention of CDISV apart from their influence on intention through LTO. This mediation analysis further uncovers the role of LTO as an important mechanism to reduce CDISV.

### 5.2. Contributions to research

This study made several contributions to the literature on IS security behaviour. First, in view of the possible delayed consequences of CDISV, we investigated the phenomenon from a temporal perspective. Previous relevant research has identified important factors, such as fear of IS threats (Johnston and Warkentin 2010), cost of noncompliance (Bulgurcu, Cavusoglu, and Benbasat 2010), and neutralisation techniques such as denial of injury (Siponen and Vance 2010), which involve an evaluation of the behaviour consequence. However, the existing research has not yet examined the possibility that individuals may have different estimations of the immediate consequence and the delayed consequence. Since CDISV usually does not cause immediate harm to organisations, such as using an easy-to-guess password, employees may underestimate the seriousness of their behaviour and thereby lead to CDISV. Based on the temporal perspective, we identified a set of constructs that are future and long-term orientated. Our results show that these constructs do influence employees' CDISV decisions. Our temporal perspective provided a new avenue for future research to identify additional constructs and relationships regarding CDISV.

Second, by adopting the temporal perspective, to our knowledge, we were the first to empirically investigate the role of LTO in the context of an employee's CDISV in an organisation. We highlighted that LTO may have important implications for future IS security behaviour research. A first research opportunity related to LTO concerns the mixed findings of the studies based on the deterrence theory in IS (D'Arcy and Herath 2011). Researchers in criminology have revealed that sanction threats are weak for those criminal offenders who do not consider future consequences since they have a tendency to deliberatively devalue the future or fail to consider the future (Nagin and Pogarsky 2004). Therefore, we suggest that future research should investigate whether or not LTO moderates the role of deterrence or monitoring employees' IS security behaviour.

A second research opportunity related to LTO is to investigate how long the delayed consequences will unfold in an individual's mind, and the role of such on IS security behaviour. According to the construal level theory, the psychological temporal distance changes people's responses to future events by changing the way people mentally represent those events (Liberman, Trope, and Wakslak 2007; Trope and Liberman 2003). In other words, people may think and behave in different patterns according to the psychologically near or distant delayed consequences. Future research can examine if this psychological, temporal distance leads to different explanations for security-related behaviours. Previous research has found that influential factors, such as value or abstractness of information, play different roles in behaviours or intentions for near and distant future events (Nussbaum, Liberman, and Trope 2006). Future IS security behaviour research can explore if similar factors exist.

A third research opportunity regarding LTO is to identify the appropriate organisational strategies that facilitate employees to generate LTO. Although we have shown that LTO can increase employees' secure behaviour, the questions still remain as to what strategies organisations should implement. Liang, Xue, and Wu (2013) suggested that organisations could adopt two types of strategies to regulate employees' IS security behaviour: promotion focus and prevention focus (Higgins 1997). Promotion focus is driven by the need for growth and development (Johnson and Yang 2010; Liang, Xue, and Wu 2013). Steidle, Gockel, and Werth (2013) found that growth needs are more likely to be fulfilled by promotion focus strategies rather than prevention focus strategies. Since we found that LTO is motivated by growth needs fulfilment, future research can examine if a promotion focus regulation strategy can increase employees' LTO.

Our third contribution is that we were the first to draw on the stewardship theory to offer a theoretical explanation and empirical support for the influential factors associated with employees' CDISV. Previous studies have dominantly applied theories such as the deterrence theory and the rational choice theory, which hold assumptions that employees are individualistic, opportunistic, and self-serving (Siponen and Vance 2014). Under such assumptions, only those factors that attach to an individual's self-utilities, such as punishment or momentary and time benefits, are found (Bulgurcu, Cavusoglu, and Benbasat 2010; D'Arcy, Hovav, and Galletta 2009). However, little research has considered the possibility that employees can be collectivists, pro-organisational, and trustworthy, as the stewardship theory assumes.

The stewardship theory provides an alternative understanding of employees' behaviour in an organisation, suggesting that employees may willingly subjugate their personal interests to protect the organisation's long-term welfare (Hernandez 2012) and may be motivated by higher-order needs such as growth, achievement, and self-actualisation as well as by intrinsic rewards (Davis, Schoorman, and Donaldson 1997). The stewardship theory is in line with our temporal perspective, suggesting that employees may generate long-term related mindsets, beliefs, and needs in an organisation, which can drive pro-organisational behaviour. Drawing on the stewardship theory, we argued that LTO, value identification, trusted relationship fulfilment, and growth needs fulfilment are important factors influencing employees' intention of CDISV. Our findings provide strong empirical support for our arguments. We believe that the stewardship theory can contribute more to IS security behaviour research. Other research fields based on the stewardship theory have suggested that factors such as psychological ownership, affective commitment (Hernandez 2012), and organisational culture (Davis, Schoorman, and Donaldson 1997) can influence employees' behaviour. Future research can examine their roles in explaining IS security behaviour.

### 5.3. Implications for practice

Our results have a number of implications for organisations to manage CDISV. We found that when employees generate a LTO, they are more likely to avoid CDISV. Therefore, a general implication is that when organisations make IS security policies, they can highlight that IS security is a long-term mission. Employees should be informed that potential threats might appear after a period of time and should pay attention to if their behaviours could cause potential threats in the future. Since LTO is composed of continuity, futurity and perseverance, we have three respective practical advices for IS security management. First, by analysing the computer logs, IT department can send a periodic report to individuals and highlight the duration for an employee to keep a secure state. In this way, employees can be aware that if they have a continuous compliance. Second, organisations should trace and analyse the long-term consequences of security incidents, noticing employees to focus on the future outcomes of their current behaviours. Third, organisations should evaluate and report the potential cost saved in managing employees' security-related behaviours, letting employees realise the value of their efforts.

Second, since we found that an employee's identification with IS security policies and recommended security behaviours can increase LTO, we suggest IS security management to design training programmes to have employees recognise the legitimacy of IS security policies. On the one hand, make employees understand the value of persistent, secure behaviour. On the other hand, IS security managers can persuade employees to not trust luck with their problematic behaviour every single time. Employees should know they play important roles in their organisations in terms of protecting against information security threats.

Third, our findings also indicate that fulfilment of higher-order needs can increase LTO. Since people care if they are trustworthy in the eyes of others, information systems can embed social features to elicit secure intentions and behaviours. An exemplary study was undertaken to incorporate social presence as a feature of UI artefacts in designing an information system (Vance et al. 2015). In their study, by showing users' current online activities, employees suppress the behaviours that are viewed as socially unacceptable. Information systems can also consider adding labels to users to reflect the security level of their behaviours.

Fourth, fulfilment of growth needs was confirmed to increase LTO in our study. IS designers can rely on logged user data and apply user modelling techniques (Schreck 2003) and learning on demand approach (Fischer 1991) to identify the opportunities to learn security knowledge that are relevant to employees' task. These approaches are useful in personalising learning opportunities for each employee and help them to learn in actual security problem situations. In addition, organisations should encourage employees to identify and report security flaws, and grant rewards appropriately if they can solve the problem by themselves.

### 5.4. Limitations

This study had several limitations. First, although CDISV was the key focus, we measured intention as the dependent variable instead of actual behaviour. The intention is regarded as a strong predictor of actual behaviour (Fishbein and Ajzen 1975), and numerous IS security behaviour studies have measured intention instead of actual behaviour (D'Arcy, Hovav, and Galletta 2009; Siponen and Vance 2010). Still, future research could make a valuable contribution by making efforts to collect data of actual behaviour. This approach would improve the credibility of the research model and provide more solid evidence for practices. Regarding a second limitation, this study used three hypothetical scenarios to measure CDISV. However, CDISV is not limited to these specific scenarios. Future research could include more types of CDISV to further test the proposed model. Third, although this study focused on CDISV, our research model may provide explanations for other types of security behaviour as well. For example, security assurance behaviour, defined by Guo (2013) as the intentional behaviours that employees actively carry out to protect the organisation's information systems, is an active and pro-organisational behaviour. Future research could examine whether or not our research model can generalise to security assurance behaviour.

## 6. Conclusion

Employees' CDISV represents a significant concern of organisations regarding IS security. Some CDISVs may not cause immediate damage to an organisation's IS, but negative consequences may unfold in the future. Without considering the delayed consequences of CDISV, employees may underestimate the seriousness of their risky behaviour. Previous research has not used the temporal perspective to examine IS security behaviour. To fill the gap, our study discussed the role of the delayed consequences of CDISV and highlighted LTO as an important factor that influences employees' decisions of CDISV. Drawing on the stewardship theory, we justified the rationality of occurrence of LTO and also identified three antecedents of LTO: value identification, trusted relationship fulfilment, and growth needs fulfilment. The empirical results supported our arguments well. Our study contributes to IS security behaviour literature by being the first to empirically investigate LTO and the first to draw on the stewardship theory in the security context. We also contribute to practice by suggesting that organisations evaluate employees' long-term performance regarding IS security and encourage them to train themselves to develop the abilities needed to solve security problems.

## Notes

1. SmartPLS 3.2.7 used in this study returns results of $d_{G1}$ and $d_{G2}$. In line with the publication by Dijkstra and Henseler (2015), $d_{G1}$ calculates the eigenvalues based on $S^{-1}\Sigma$, whereby $S$ represents the sample covariance matrix and $\Sigma$ the model-implied covariance matrix. In contrast, $d_{G2}$ uses a corrected eigenvalue computation based on $S^{-1/2}\ \Sigma\ S^{-1/2}$.
2. Within the framework of marker-variable analysis, a method factor is assumed to have a constant correlation with all of the measured items. Under this assumption, a CMV-adjusted correlation between the variables under investigation, $r_a$, will be computed by partialling out $r_m$, from the uncorrected correlation, $r_u$. In particular, with a sample size of n, $r_a$ and its $t$-statistic can be calculated as follows: $r_a = (r_u - r_m)/(1 - r_m)$, $t = r_a/\mathrm{sqr}(1 - {r_a}^2)/(n-3)$.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Funding

This work was supported by China Ministry of Education of Humanities and Social Science project: [Grant Number 17YJC630072]; China Postdoctoral Science Foundation: [Grant Number 2016M601315]; Doctoral Scientific Research Foundation of Liaoning Province: [Grant Number 20170520435]; National Natural Science Foundation of China: [Grant Number 71421001,71431002]; Fundanmental Research Funds for the Central Universities [Grant Number DUT18RC(4)037].

## References

Ajzen, I. 1988. *Attitudes, Personality, and Behaviour*. Buckingham: Open University Press.

Alderfer, C. P. 1972. *Existence, Relatedness, and Growth: Human Needs in Organizational Settings*. New York: Free Press. doi:10.2307/2063565.

Armstrong, D. J., and B. C. Hardgrave. 2007. "Understanding Mindshift Learning: The Transition to Object-Oriented Development." *MIS Quarterly* 31 (3): 453–474. doi:10.2307/25148803.

Au, N., E. W. T. Ngai, and T. C. E. Cheng. 2008. "Extending the Understanding of End User Information Systems Satisfaction Formation: An Equitable Needs Fulfillment Model Approach." *MIS Quarterly* 32 (1): 43–66. doi:10.2307/25148828.

Bateman, P. J., P. H. Gray, and B. S. Butler. 2011. "Research Note—the Impact of Community Commitment on Participation in Online Communities." *Information Systems Research* 22 (4): 841–854. doi:10.1287/isre.1090.0265.

Bearden, W. O., R. R. Money, and J. L. Nevins. 2006. "A Measure of Long-Term Orientation: Development and Validation." *Journal of the Academy of Marketing Science* 34 (3): 456–467. doi:10.1177/0092070306286706.

Becker, J. M., K. Klein, and M. Wetzels. 2012. "Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models." Long Range Planning 45 (5-6): 359–394. doi:10.1016/j.lrp.2012.10.001.

Besharov, M. L. 2014. "The Relational Ecology of Identification: How Organizational Identification Emerges When Individuals Hold Divergent Values." *Academy of Management Journal* 57 (5): 1485–1512. doi:10.5465/amj.2011.0761.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors." MIS Quarterly 39 (4): 837–864. doi:10.2530.

Brigham, K. H., G. T. Lumpkin, G. T. Payne, and M. A. Zachary. 2014. "Researching Long-Term Orientation." *Family Business Review* 27 (1): 72–88. doi:10.1177/0894486513508980.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. "Information Security Policy Compliance: An Empirical

Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–548. doi:10.2307/25750690.

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling." *MIS Quarterly* 22 (1): vii–xvi.

Chin, W. W., J. B. Thatcher, and R. T. Wright. 2012. "Assessing Common Method Bias: Problems with the ULMC Technique." *MIS Quarterly* 36 (3): 1003–1019. doi:10.1287/isre.1070.0123.

D'Arcy, J., and T. Herath. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings." *European Journal of Information Systems* 20 (6): 643–658. doi:10.1057/ejis.2011.23.

D'Arcy, J., A. Hovav, and D. Galletta. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research* 20 (1): 79–98. doi:10.1287/isre.1070.0160.

Das, T. K., and B. S. Teng. 1997. "Time and Entrepreneurial Risk Behavior." *Entrepreneurship Theory and Practice* 22 (2): 69–88. doi:10.1177/104225879802200206.

Davis, J. H., F. D. Schoorman, and L. Donaldson. 1997. "Toward a Stewardship Theory of Management." *Academy of Management Review* 22 (1): 20–47. doi:10.2307/259223.

Deci, E. L., and R. Flaste. 1995. *Why We Do What We Do: The Dynamics of Personal Autonomy*. New York: GP Putnam's Sons.

Deci, E. L., R. J. Vallerand, L. G. Pelletier, and R. M. Ryan. 1991. "Motivation and Education: The Self-Determination Perspective." *Educational Psychologist* 26 (3–4): 325–346. doi:10.1080/00461520.1991.9653137.

Deloitte. 2013. "Blurring the Lines: 2013 TMT global security study." Accessed March 22, 2018. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/dttl_TMT_GlobalSecurityStudy_English_final_020113.pdf.

Dijkstra, T. K., and J. Henseler. 2015. "Consistent and Asymptotically Normal PLS Estimators for Linear Structural Equations." *Computational Statistics & Data Analysis* 81: 10–23. doi:10.1016/j.csda.2014.07.008.

Fischer, G. 1991. "Supporting Learning on Demand with Design Environments." In *Proceedings of the International Conference on the Learning Sciences*, vol. 199, edited by Lawrence Birnbaum, 165–172. Charlottesville, VA: Association for the Advancement of Computing in Education.

Fishbein, M., and I. Ajzen. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Flowerday, S., and R. von Solms. 2005. "Real-Time Information Integrity=System Integrity+ Data Integrity+ Continuous Assurances." *Computers & Security* 24 (8): 604–613. doi:10.1016/j.cose.2005.08.004.

Fornell, C., and D. F. Larcker. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics." *Journal of Marketing Research* 18 (3): 382–388. doi:10.2307/3150980.

Gefen, D., and D. Straub. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example." *Communications of the Association for Information Systems* 16 (1): 91–109.

Graso, M., and T. M. Probst. 2012. "The Effect of Consideration of Future Consequences on Quality and Quantity Aspects of Job Performance1." *Journal of Applied Social Psychology* 42 (6): 1335–1352. doi:10.1111/j.1559-1816.2012.00901.x.

Guo, Ken H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis." *Computers & Security* 32: 242–251. doi:10.1016/j.cose.2012.10.003.

Hair Jr, J. F., L. M. Matthews, R. L. Matthews, and M. Sarstedt. 2017. "PLS-SEM or CB-SEM: Updated Guidelines on Which Method to Use." *International Journal of Multivariate Data Analysis* 1 (2): 107–123. doi.org/10.1504/ijmda.2017.087624.

Henseler, J., T. K. Dijkstra, M. Sarstedt, C. M. R. A. Diamantopoulos, D. W. Straub, D. J. Ketchen Jr, J. F. Hair, G. T. M. Hult, and R. J. Calantone. 2013. Common Beliefs and Reality About PLS." *Organizational Research Methods* 17 (2): 182–209. doi.org/10.1177/1094428114526928.

Henseler, J., G. Hubona, and P. A. Ray. 2016. "Using PLS Path Modeling in New Technology Research: Updated Guidelines." *Industrial Management & Data Systems* 116 (1): 2–20. doi.org/10.1108/imds-09-2015-0382.

Herath, T., and H. R. Rao. 2009. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness." *Decision Support Systems* 47 (2): 154–165. doi:10.1016/J.Dss.2009.02.005.

Hernandez, M. 2012. "Toward an Understanding of the Psychology of Stewardship." *Academy of Management Review* 37 (2): 172–193. doi:10.5465/amr.2010.0363.

Hershfield, H. E., T. R. Cohen, and L. Thompson. 2012. "Short Horizons and Tempting Situations: Lack of Continuity to Our Future Selves Leads to Unethical Decision Making and Behavior." *Organizational Behavior and Human Decision Processes* 117 (2): 298–310. doi:10.1016/j.obhdp.2011.11.002.

Higgins, E. T. 1997. "Beyond Pleasure and Pain." *American Psychologist* 52 (12): 1280–1300. doi:10.1037/0003-066x.52.12.1280.

Hofstede, G. 1991. *Cultures and Organizations. Intercultural Cooperation and Its Importance for Survival. Software of the Mind*. London: Mc Iraw-Hill.

Hu, L., and P. M. Bentler. 1998. "Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification." *Psychological Methods* 3 (4): 424–453. doi.org/10.1037//1082-989x.3.4.424.

Johnson, R. E., and L. Q. Yang. 2010. "Commitment and Motivation at Work: The Relevance of Employee Identity and Regulatory Focus." *Academy of Management Review* 35 (2): 226–245. doi:10.5465/amr.2010.48463332.

Johnston, A. C., and M. Warkentin. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study." *MIS Quarterly* 34 (3): 549–566. doi:10.2307/25750691.

Joireman, J., D. Kamdar, D. Daniels, and B. Duell. 2006. "Good Citizens to the End? It Depends: Empathy and Concern with Future Consequences Moderate the Impact of a Short-Term Time Horizon on Organizational Citizenship

Behaviors.” *Journal of Applied Psychology* 91 (6): 1307–1320. doi:10.1037/0021-9010.91.6.1307.

Kahneman, D., and A. Tversky. 1979. “Prospect Theory: An Analysis of Decision Under Risk.” *Econometrica* 47 (2): 263–291. doi:10.2307/1914185.

Karniol, R., and M. Ross. 1996. “The Motivational Impact of Temporal Focus: Thinking About the Future and the Past.” *Annual Review of Psychology* 47 (1): 593–620. doi:10.1146/annurev.psych.47.1.593.

Keough, K. A., P. G. Zimbardo, and J. N. Boyd. 1999. “Who’s Smoking, Drinking, and Using Drugs? Time Perspective as a Predictor of Substance Use.” *Basic and Applied Social Psychology* 21 (2): 149–164. doi:10.1207/15324839951036498.

Komorita, S. S., and C. D. Parks. 1994. *Social Dilemmas*. Madison: Brown & Benchmark.

Le Breton-Miller, I., and D. Miller. 2011. “Commentary: Family Firms and the Advantage of Multitemporality.” *Entrepreneurship Theory and Practice* 35 (6): 1171–1177. doi:10.1111/j.1540-6520.2011.00496.x.

Leonard, L. N. K., and T. P. Cronan. 2005. “Attitude Toward Ethical Behavior in Computer Use: A Shifting Model.” *Industrial Management & Data Systems* 105 (9): 1150–1171. doi:10.1108/02635570510633239.

Liang, H., Y. Xue, and L. Wu. 2013. “Ensuring Employees’ IT Compliance: Carrot or Stick?” *Information Systems Research* 24 (2): 279–294. doi:10.1287/isre.1120.0427.

Liberman, N., Y. Trope, and C. Wakslak. 2007. “Construal Level Theory and Consumer Behavior.” *Journal of Consumer Psychology* 17 (2): 113–117. doi:10.1016/s1057-7408(07)70017-7.

Lindell, M. K., and D. J. Whitney. 2001. “Accounting for Common Method Variance in Cross-Sectional Research Designs.” *Journal of Applied Psychology* 86 (1): 114–121. doi:10.1037/0021-9010.86.1.114.

Loch, K. D., and S. Conger. 1996. “Evaluating Ethical Decision Making and Computer Use.” *Communications of the ACM* 39 (7): 74–83. doi:10.1145/233977.233999.

Lumpkin, G. T., and K. H. Brigham. 2011. “Long-Term Orientation and Intertemporal Choice in Family Firms.” *Entrepreneurship Theory and Practice* 35 (6): 1149–1169. doi:10.1111/j.1540-6520.2011.00495.x.

Lumpkin, G. T., K. H. Brigham, and T. W. Moss. 2010. “Long-Term Orientation: Implications for the Entrepreneurial Orientation and Performance of Family Businesses.” *Entrepreneurship and Regional Development* 22 (3-4): 241–264. doi:10.1080/08985621003726218.

Mael, F., and B. E. Ashforth. 1992. “Alumni and Their Alma Mater: A Partial Test of the Reformulated Model of Organizational Identification.” *Journal of Organizational Behavior* 13 (2): 103–123. doi:10.1002/job.4030130202.

Malhotra, N. K., S. S. Kim, and A. Patil. 2006. “Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research.” *Management Science* 52 (12): 1865–1883. doi:10.1287/mnsc.1060.0597.

Mannix, E. A. 1991. “Resource Dilemmas and Discount Rates in Decision Making Groups.” *Journal of Experimental Social Psychology* 27 (4): 379–391. doi:10.1016/0022-1031(91)90032-2.

Mannix, E. A., and G. F. Loewenstein. 1993. “Managerial Time Horizons and Interfirm Mobility: An Experimental Investigation.” *Organizational Behavior and Human Decision Processes* 56 (2): 266–284. doi:10.1006/obhd.1993.1055.

Mannix, E. A., C. H. Tinsley, and M. Bazerman. 1995. “Negotiating Over Time: Impediments to Integrative Solutions.” *Organizational Behavior and Human Decision Processes* 62 (3): 241–251. doi:10.1006/obhd.1995.1047.

Maslow, A. H., R. Frager, J. Fadiman, C. McReynolds, and R. Cox. 1970. *Motivation and Personality*. New York: Harper & Row.

McClelland, D. C., and G. Teague. 1975. “Predicting Risk Preferences among Power Related Tasks.” Journal of Personality 43 (2): 266–285. doi:10.1111/j.1467-6494.1975.tb00706.x.

Miller, D., and I. Le Breton-Miller. 2005. *Managing for the Long Run: Lessons in Competitive Advantage from Great Family Businesses*. Boston: Business Press.

Miller, D., and J. Shamsie. 2001. “Learning Across the Life Cycle: Experimentation and Performance among the Hollywood Studio Heads.” *Strategic Management Journal* 22 (8): 725–745. doi:10.1002/smj.171.

Moss, T. W., G. T. Payne, and C. B. Moore. 2014. “Strategic Consistency of Exploration and Exploitation in Family Businesses.” *Family Business Review* 27 (1): 51–71. doi:10.1177/0894486513504434.

Mowday, R. T., L. W. Porter, and R. M. Steers. 2013. *Employee—Organization Linkages: The Psychology of Commitment, Absenteeism, and Turnover*. New York: Academic press.

Nagin, D. S., and R. Paternoster. 1993. “Enduring Individual Differences and Rational Choice Theories of Crime.” *Law and Society Review* 27 (3): 467–496. doi:10.2307/3054102.

Nagin, D. S., and G. Pogarsky. 2001. “Integrating Celerity, Impulsivity, and Extralegal Sanction Threats Into a Model of General Deterrence: Theory and Evidence.” Criminology 39 (4): 865–892. doi:10.1111/crim.2001.39.issue-4.

Nagin, D. S., and G. Pogarsky. 2004. “Time and Punishment: Delayed Consequences and Criminal Behavior.” *Journal of Quantitative Criminology* 20 (4): 295–317. doi:10.1007/s10940-004-5866-1.

Nitzl, C., J. L. Roldan, and G. Cepeda. 2016. “Mediation Analysis in Partial Least Squares Path Modeling.” *Industrial Management & Data Systems* 116 (9): 1849–1864. doi.org/10.1108/imds-07-2015-0302.

Nunnally, J. C. 1978. Psychometric Theory. New York: McGraw-Hill.

Nussbaum, S., N. Liberman, and Y. Trope. 2006. “Predicting the Near and Distant Future.” *Journal of Experimental Psychology: General* 135 (2): 152–161. doi:10.1037/0096-3445.135.2.152.

O’Reilly, C. A., and J. Chatman. 1986. “Organizational Commitment and Psychological Attachment: The Effects of Compliance, Identification, and Internalization on Prosocial Behavior.” *Journal of Applied Psychology* 71 (3): 492–499. doi:10.1037/0021-9010.71.3.492.

Pavlou, P. A., H. Liang, and Y. Xue. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective.” *MIS Quarterly* 31 (1): 105–136. doi:10.2307/25148783.

Petter, S., D. Straub, and A. Rai. 2007. “Specifying Formative Constructs in Information Systems Research.” *MIS Quarterly* 31 (4): 623–656. doi:10.2307/25148814.

Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.” *Journal of Applied Psychology* 88 (5): 879–903. doi:10.1037/0021-9010.88.5.879.

Ponemon. 2015. “2014: A Year of Mega Breaches.” Accessed March 22, 2018. https://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

Ponemon. 2018a. “2018 Cost of Insider Threats Global Organizations.” Accessed August 22, 2018. https://www.observeit.com/ponemon-report-cost-of-insider-threats/.

Ponemon. 2018b. “2018 Cost of a Data Breach Study.” Accessed August 22, 2018. https://www.ibm.com/security/data-breach?cm_mc_uid=15296272607515349207711&cm_mc_sid_50200000=47261451534920771172&cm_mc_sid_52640000=41899621534920771174.

Prahalad, C. K., and R. A. Bettis. 1986. “The Dominant Logic: A New Linkage between Diversity and Performance.” *Strategic Management Journal* 7 (6): 485–501. doi:10.1002/smj.4250070602.

Pratt, T. C., F. T. Cullen, K. R. Blevins, L. E. Daigle, and T. D. Madensen. 2006. “The Empirical Status of Deterrence Theory: A Meta-Analysis.” In *Taking Stock: The Status of Criminological Theory*, vol.15, edited by Francis T. Cullen, John Paul Wright, and Kristie R. Blevins, 367–396. New Brunswick, NJ: Transaction.

Preacher, K. J., and A. F. Hayes. 2008. “Asymptotic and Resampling Strategies for Assessing and Comparing Indirect Effects in Multiple Mediator Models.” *Behavior Research Methods* 40 (3): 879–891. doi.org/10.3758/brm.40.3.879.

Richardson, H. A., M. J. Simmering, and M. C. Sturman. 2009. “A Tale of Three Perspectives.” *Organizational Research Methods* 12 (4): 762–800. doi:10.1177/1094428109332834.

Ringle, C. M., M. Sarstedt, and D. W. Straub. 2012. “A Critical Look at the Use of PLS-SEM in MIS Quarterly.” *MIS Quarterly* 36 (1): iii–xiv.

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

Schoemaker, P. J. H. 1982. “The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations.” *Journal of Economic Literature* 20 (2): 529–563.

Schreck, J. 2003. *Security and Privacy in User Modeling*. Dordrecht: Springer. doi:10.1007/978-94-017-0377-2.

Sinclair, J. 2003. *Collins COBUILD English Dictionary for Advanced Learners*. Glasgow: HarperCollins Publishers.

Siponen, M., and A. Vance. 2010. “Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations.” *MIS Quarterly* 34 (3): 487–502. doi:10.2307/25750688.

Siponen, M., and A. Vance. 2014. “Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations.” *European Journal of Information Systems* 23 (3): 289–305. doi:10.1057/ejis.2012.59.

Sivo, S. A., C. Saunders, Q. Chang, and J. J. Jiang. 2006. “How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research.” *Journal of the Association for Information Systems* 7 (6): 351–414. doi:10.17705/1jais.00093.

Steidle, A., C. Gockel, and L. Werth. 2013. “Growth or Security? Regulatory Focus Determines Work Priorities.” *Management Research Review* 36 (2): 173–182. doi:10.1108/01409171311292261.

Strathman, A., F. Gleicher, D. S. Boninger, and C. S. Edwards. 1994. “The Consideration of Future Consequences: Weighing Immediate and Distant Outcomes of Behavior.” *Journal of Personality and Social Psychology* 66 (4): 742–752. doi:10.1037/0022-3514.66.4.742.

Straub, D. W., and R. J. Welke. 1998. “Coping with Systems Risk: Security Planning Models for Management Decision Making.” *MIS Quarterly* 22 (4): 441–469. doi:10.2307/249551.

Sumo, R., W. van der Valk, A. van Weele, and C. Bode. 2016. “Fostering Incremental and Radical Innovation Through Performance-Based Contracting in Buyer-Supplier Relationships.” *International Journal of Operations & Production Management* 36 (11): 1482–1503. doi.org/10.1108/ijopm-05-2015-0305.

Takemura, T., and A. Komatsu. 2012. “*Who Sometimes Violates the Rule of the Organizations? An Empirical Study on Information Security Behaviors and Awareness.*” Paper presented at the workshop on the economics of information security, Berlin, June 25–26.

Trope, Y., and N. Liberman. 2003. “Temporal Construal.” *Psychological Review* 110 (3): 403–421. doi:10.1037/0033-295X.110.3.403.

Vance, A., P. B. Lowry, and D. Eggett. 2015. “Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations.” MIS Quarterly 39 (2): 345–366. doi:10.2530.

Vinzi, V. E., W. W. Chin, J. Henseler, and H. Wang. 2010. Handbook of Partial Least Squares: Concepts, Methods and Applications. Heidelberg, Dordrecht, London, New York: Springer.

Vroom, C., and R. von Solms. 2004. “Towards Information Security Behavioural Compliance.” *Computers & Security* 23 (3): 191–198. doi:10.1016/j.cose.2004.01.012.

Wang, T. Y., and P. Bansal. 2012. “Social Responsibility in New Ventures: Profiting From a Long-Term Orientation.” *Strategic Management Journal* 33 (10): 1135–1153. doi:10.1002/smj.1962.

Warkentin, M., K. Davis, and E. Bekkering. 2004. “Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security.” *Journal of Organizational and End User Computing* 16 (3): 41–58. doi:10.4018/joeuc.2004070103.

Wetzels, M., G. Odekerken-Schröder, and C. van Oppen. 2009. “Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration.” *MIS Quarterly* 33 (1): 177–195. doi:10.2307/20650284.

Williams, L. J., N. Hartman, and F. Cavazotte. 2010. “Method Variance and Marker Variables: A Review and Comprehensive CFA Marker Technique.” *Organizational Research Methods* 13 (3): 477–514. doi:10.1177/1094428110366036.

Zahra, S. A. 2005. “Entrepreneurial Risk Taking in Family Firms.” *Family Business Review* 18 (1): 23–40. doi:10.1111/j.1741-6248.2005.00028.x.

Zhao, X., J. G. Lynch Jr, and Q. Chen. 2010. “Reconsidering Baron and Kenny: Myths and Truths about Mediation

Analysis." *Journal of Consumer Research* 37 (2): 197–206. doi.org/10.1086/651257.

Zimbardo, P. G., K. A. Keough, and J. N. Boyd. 1997. "Present Time Perspective as a Predictor of Risky Driving." *Personality and Individual Differences* 23 (6): 1007–1023. doi:10.1016/s0191-8869(97)00113-x.

## Appendices

### Appendix A. Scenarios

In the scenarios, we describe a situation that Newman, an employee of your company, is facing. Please read the scenario carefully first, and then indicate the extent to which you agree with the following statements.

#### Scenario 1. Unauthorised portable devices for storing corporate data

Newman wants to copy a file and show it to clients at their meeting. A personal unencrypted USB stick is available nearby. The file contains the contract draft. However, the meeting is starting soon, and it takes time to find an encrypted USB stick. Newman decides to copy the file into the personal unencrypted USB stick.

#### Scenario 2. Sending unencrypted emails

Newman needs to send an encrypted email to a client. The client says that she has difficulties decrypting the email and asks Newman to send her an unencrypted one. The file contains the contract draft. However, the client says that, if she cannot open the email, she may consider switching to another company. So, Newman decides to send an unencrypted email to her.

#### Scenario 3. Downloading suspicious files from the internet

Newman needs to search for some information from the Internet in order to complete some work. A file on a website is thought to contain the required information, but Newman is unsure that the site is trustworthy. The browser also displays a security warning stating that 'this file type can potentially harm your computer.' However, it takes time to find the information by other means, and the file helps to complete the work more quickly. Newman decides to download it.

### Appendix B. Survey questions

Following each scenario, respondents were presented with the following questions. Each respondent was randomly assigned one scenario. The item wordings were slightly modified to fit each scenario. The expression of 'the behaviour' refers to Newman's action as described in the scenario above.

*Intention of CDISV (INT)* (D'Arcy, Hovav, and Galletta 2009*)*

If you were Newman, what is the likelihood that you would have copied the file into a personal unencrypted USB stick?

I could see myself copying the file into a personal unencrypted USB stick if I were in Newman's situation.

*Continuity (LTO_C)* (Brigham et al. 2014*)*

It is valuable that I always avoid the behaviour without exception.

Avoiding the behaviour all the time at work is of great worth.

*Futurity (LTO_F)* (Brigham et al. 2014*)*

In the long run, it is helpful for my organization to evaluate the consequences of such type of behaviour.

In the long run, it is valuable for my organization to notice the possible negative consequences caused by such type of behaviour.

*Perseverance (LTO_P)* (Brigham et al. 2014*)*

I do not mind giving up the current convenience if it could ensure my organization's information security.

I do not mind extra work if it could ensure my organization's information security.

*Value identification (VI)* (Davis, Schoorman, and Donaldson 1997*)*

I think it is accepted that my organization discourages the behaviour.

I fully understand the necessity of avoiding the behaviour in my organization.

*Trusted relationship fulfilment (TRF)* (Deci et al. 1991)

If my co-workers knew that I avoided the behaviour, they might recognize me as a trustworthy co-worker.

If my colleagues knew that I avoided the behaviour, they might recognize me as a responsible co-worker.

*Growth needs fulfilment (GNF)* (Alderfer 1972*)*

It is an opportunity for me to master more information protection skills, if I find alternative secure ways to do the work.

It is an opportunity for me to learn more information security knowledge, if I find alternative secure ways to do the work.

It is an opportunity for me to show my talents in solving information security problems, if I find alternative secure ways to do the work.