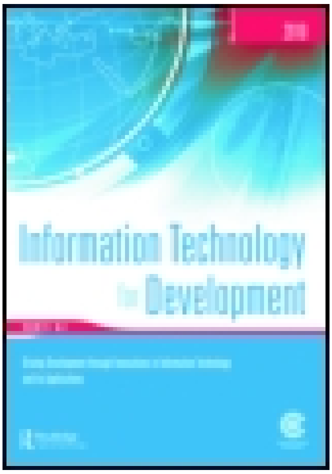


Information Technology for Development
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/titd20

The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru

Jaehun Joo[a] & Anat Hovav[b]

[a] Department of Information Management, Dongguk University, 707 Sukjang-dong, Gyeongbuk 780-714, Gyeongju-si, Republic of Korea

[b] Korea University Business School, 324 LG-Posco Anam-Dong, Seoul 136-701, Republic of Korea

Published online: 13 Jan 2015.

To cite this article: Jaehun Joo & Anat Hovav (2015): The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru, Information Technology for Development, DOI: 10.1080/02681102.2014.979393

To link to this article: http://dx.doi.org/10.1080/02681102.2014.979393

Information Technology for Development, 2015
http://dx.doi.org/10.1080/02681102.2014.979393

Routledge
Taylor & Francis Group

The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru

Jaehun Joo[a] and Anat Hovav[b*]

[a]Department of Information Management, Dongguk University, 707 Sukjang-dong, Gyeongbuk 780-714, Gyeongju-si, Republic of Korea; [b]Korea University Business School, 324 LG-Posco Anam-Dong, Seoul 136-701, Republic of Korea

This study analyzes the determinants of information security that influence the adoption of Web-based integrated information systems (IIS) by government agencies in Peru. The study introduces Web-based information systems designed to formulate strategic plans for the Peruvian government. A theoretical model is proposed to test the impact of organizational factors such as deterrent efforts, severity efforts, and preventive efforts and individual factors such as perceived information security threats and security awareness on intentions to use Web-based IIS. The empirical results indicate that deterrent efforts and deterrent severity have no significant influence on use intentions of IIS, whereas preventive efforts play an important role in such intentions. Information security awareness and perceived information security threats as individual factors have a significant effect on intentions to use the system. This suggests that organizations should implement preventive efforts by introducing various information security solutions, and improve information security awareness while reducing perceived information security threats.

Keywords: information security; deterrent and preventive efforts; information security awareness; information security threats; e-government; Peru

1. Introduction

Prior studies on the implementation of e-government have addressed a number of challenges such as trust (Lee & Levy, 2014), gender and education, and the digital divide. E-government studies also examined the implementation of security and privacy policies and frameworks in various countries (e.g. see Wangwe, Eloff, & Venter, 2012; Wu, 2014). In addition, studies have examined users' perceptions of security on intention to use an online shopping system (Lian & Lin, 2008) and on perceived risk (see Bhatnagar, Misra, & Rao, 2000; Kim, Ferrin, & Rao, 2008). These studies surveyed external users (in a B-2-C context) and operationalized perception of security based on the traditional CIA (confidentiality, integrity, and availability) construct (see Hartono, Holsapple, Kim, & Simpson, 2014).

Yet, to date, none of these studies examined internal e-government users' security perceptions and awareness influence on intention to use the system. In an environment when local and regional government entities are not mandated to adopt federal e-government systems, security concerns may be a major hindrance of adoption. In 2010, the Peruvian government engaged the Korea Development Institute (KDI) to facilitate the installation of a web-based integrated information system (IIS).

The adoption of e-government in South America lags behind that of North America, Asia, and Europe (UN, 2012). Furthermore, Peru's information and communications technology (ICT) maturity as of 2010 was the sixth lowest in South America (UN, 2012), while its

*Corresponding author. Email: anatzh@korea.ac.kr e-government development index is the seventh (UN, 2012). Therefore, it is not surprising that the sophistication level of the hardware, software, and telecommunication capabilities used in the Peruvian implementation of the IIS described in the later text was relatively lower than in the USA and South Korea (CEPLAN, 2010). Similarly, the level of information security applied to the implemented system does not match accepted standards as described by Zhao and Zhao (2010). In addition, a key security concern is that the infrastructure used to support the IIS system is managed by a private company. This is of major importance in an environment where corruption is a common occurrence. Peru's freedom from corruption index (34.0) is significantly below the world average.[1]

The challenges and opportunities of the adoption of a Web-based IIS have been discussed extensively (see Carstensen & Vogelsang, 2001; Khan & Qureshi, 2009; Yao, 2008; Zhao & Zhao, 2010). Although the benefits of Web-based IIS are recognized, they can be vulnerable to information security threats (Smith & Jamieson, 2006). Such threats are more likely to occur in environments where the technical and human-resource infrastructures are lacking such as in transition or developing economies (Wangwe et al., 2012). The goal of this study is to identify organizational and individual factors that might affect the adoption of an e-government system in the context of a developing county such as Peru. The factors related to information system security issues draw on general deterrence theory, user attitude towards security, and fear appeal theory (Johnston & Warkentin, 2010; Kankanhalli, Teo, Tan, & Wei, 2003; Siponen, 2000; Straub 1990). The research model and hypotheses put forth are tested by using data collected from users working for national and regional government agencies in Peru.

This paper is organized as follows. Section 2 outlines the prior literature on information security effectiveness. Section 3 describes the IIS. Sections 4 and 5 outline the research hypotheses, and methodology. We end with a discussion of the results, implications for academia and practice, and conclusions.

2. Literature review and theoretical framework

Previous studies have typically focused on several factors that influence information security effectiveness. In particular, deterrent efforts, deterrent severity, preventive efforts, and information security awareness and threats have been investigated. While early studies measured deterrence at the organizational level (see Straub, 1990), more recent research has investigated deterrence at the individual level (see D'Arcy, Hovav, & Galletta, 2009). The goal of this study is to examine the effect of deterrence on the use of an organizational system. Therefore, we measure deterrence at the organizational level. Preventive efforts are inherently the responsibility of the organization and have only been studied at the organizational level. Organizations must try to maximize their deterrence and prevention efforts to improve information systems security (Straub & Welke, 1998). Thus, we posit that efforts at the organizational level are needed to enhance the security of the IIS.

Organizational employees' information security awareness impacts their attitude and intention to comply with information security policies (Bulgurcu, Cavusoglu, & Benbasat, 2010). Information security awareness is an important part of an effective IS security management (Cavusoglu, Son, & Benbasat, 2009). Employees' perception or awareness of information security threat also plays an important role in shaping attitude toward information security and behavioral intention (Bulgurcu et al., 2010). Thus, in addition to the aforementioned organizational factors, effective information security management depends on individual factors such as users' awareness and their perceived threat (D'Arcy et al., 2009; Yeh & Chang, 2007). User awareness is of particular interest since it was found to be culturally dependent (Hovav &

D’Arcy, 2012). The second factor, perceived threat, comes from fear appeal theory (Johnston & Warkentin, 2010). This factor is also of particular interest given Peru’s culture (for further details, see discussion later in the text).

2.1. *Organizational factors: general deterrence theory*

General deterrence theory posits that people will not commit crimes when the risk of getting caught (certainty of sanction) is high and severe penalties (severity of sanction) are applied (Blumstein, 1978). Straub (1990) was the first to suggest a security impact model representing a theoretical relationship between computer abuse, deterrents, and organizational preventive efforts.

2.1.1. *Deterrent efforts*

Generally, deterrent measures are efforts to discourage people from criminal or anti-social behavior through a threat of sanctions or the administration of strong sanctions (Blumstein, 1978; Forcht, 1994; Pearson & Weiner, 1985). The certainty and harshness of punishments for such illegal or unethical acts enhance the effectiveness of sanctions (Williams & Hawkins, 1986). In the context of information security, sanctions as deterrent measures have been categorized into the certainty (e.g. probability of getting caught) and severity of sanctions (e.g. the severity of the punishment such as suspension of duties or even prosecution in court) (Kankanhalli et al., 2003).

A number of IS scholars have advocated the use of deterrence theory in security research (D’Arcy et al., 2009; Kankanhalli et al., 2003; Straub, 1990; Straub & Nance, 1990; Whitman, 2004; Yeh & Chang, 2007). Straub (1990) examined 1211 organizations and found that IS security abuse can be reduced through deterrent efforts. Straub and Welke (1998) highlighted the importance of communicating the certainty and severity of sanctions as part of employee education and training programs in minimizing security violations. Kankanhalli et al. (2003) and Whitman (2004) studied whether the use of sanctions can enhance IS security effectiveness. They found that deterrents at the organizational level (measured in man-hours spent on security efforts) can enhance IS security effectiveness and reduce the likelihood of IS abuse.

2.1.2. *Deterrent severity*

At the individual level, research on the effect of deterrent severity found contradictory (D’Arcy et al., 2009; Ifinedo, 2012) and culturally dependent (Hovav & D’Arcy, 2012) results. At the organizational level, previous studies have found that deterrent efforts are particularly effective if the punishment for IS abuse is severe (Straub, 1990). Deterrent severity corresponds to the severity of sanctions, which can dissuade people from IS security abuse (D’Arcy et al., 2009). When people are caught, they are likely to be punished severely (e.g. reprimands by management, the suspension of duties, dismissals, and prosecution) (Kankanhalli et al., 2003).

2.1.3. *Preventive measures*

When potential abusers choose to ignore deterrent measures, organizations have to strengthen the systems against their threats through the implementation of preventive measures. The main objective of preventive measures is to wear down abusers by implementing security technology (hardware or software) that can prevent unauthorized access to and use of IS assets (Straub, 1990). Preventive measures are attempts and safeguards to ward off criminal behavior through various controls (Forcht, 1994) and to enforce policy statements and guidelines (Gopal & Sanders, 1997). In other words, these safeguards limit security violations by actively enforcing the organization's security policies (Spicer, 2004). Preventive efforts include the implementation of measures for detecting, documenting, and countering potential threats (Yeh & Chang, 2007) and the deployment of advanced security software or controls for protecting IS assets, including advanced access control, intrusion detection, firewall, surveillance mechanisms, and the generation of exception reports (Kankanhalli et al., 2003).

Previous studies have found that security software can provide basic (embedded in operating systems), intermediate (embedded in database management systems), and advanced (specialized security software of access control to IS) levels of security (Kankanhalli et al., 2003; Nance & Straub, 1988; Weber, 1988). Deploying advanced security software is crucial in that such software can offer better access protection and intrusion detection through the provision of more sophisticated firewalls, and the detection of unauthorized IS activities (Kankanhalli et al., 2003).

Although some empirical studies have found that preventive efforts can create more obstacles for people engaging in IS abuse (Kankanhalli et al., 2003), others have demonstrated that they can impede business functions (Whitman, 2004) and even reduce profits (Gopal & Sanders, 1997). In this regard, Schuessler (2009) suggested that the strategic use of prevention efforts can minimize their negative impact on the firm's operations while affording the firm a desired level of protection.

2.2. *Individual factors: perceived awareness and fear appeal theory*

2.2.1. *Awareness*

User awareness is touted as a strong mechanism to reduce internal misuse and increase compliance (Whitman, 2004). Information security awareness is defined as an employee's general knowledge about information security and his or her cognizance of the organization's information security policy (Bulgurcu et al., 2010). This definition is consistent with the view that security awareness is a state in which employees are aware of and are ideally committed to their organization's security objectives (Siponen, 2000). Information security awareness forms part of information security management and ensures that all employees are aware of their role and responsibility with respect to information security (Kritzinger & Smith, 2008).

D'Arcy et al. (2009) found that organizations can use three security countermeasures: user awareness of security policies; security education, training, and awareness programs; and computer monitoring to reduce user IS abuse. They demonstrated that users' awareness of countermeasures can impact their perception of sanctions, which in turn can reduce their IS abuse intentions (D'Arcy et al., 2009). Yet, employee awareness is recognized as one of the greatest challenges in implementing security (Knapp, Morris, Marshall, & Byrd, 2009).

Ku, Chang, and Yen (2009) highlighted that employee awareness of information security is one of the key factors in the successful self-implementation of information security systems. More recently, Bulgurcu et al. (2010) found that information security awareness can directly and indirectly influence employee beliefs about their compliance with information security policy. Similarly, information security awareness is of crucial importance since information security technologies or procedures can be misused, misinterpreted, or ignored by end-users, thereby losing their real usefulness (Siponen, 2000; Siponen & Vance, 2010).

The "fear appeal" theory was first proposed by Hovland et al. (1953). Rogers's (1975) protection motivation theory (PMT) describes the "process" involved in coping with a threat rather than the threat as a behavioral motivator. Subsequent research suggests that protection motivation is composed of two processes (Maddux & Rogers, 1983). While threat appraisal is the process evaluating maladaptive behavior, coping appraisal is the process of evaluating the ability to cope with the threat. In this study, we chose to only measure the threat appraisal process for several reasons: (1) ICT is a relatively new phenomenon for the Peruvian government employees and it was unlikely that the users of the IIS would have been able to identify coping mechanisms. (2) Johnston and Warkentin (2010) suggest that the coping mechanism manifests if an individual perceive the threat to be moderate to high. Investigating a two-phase process requires a different research design than the one employed in this study. Due to the limited scope of the project, we would not have been able to create a research design that would allow us to manipulate the perceive threat and subsequently measure the resultant efficacy. (3) Peru's uncertainty avoidance index is measured at 87 (Hofstede, 2001). Uncertainty avoidance scores indicate the extent to which people from a certain culture can manage uncertainty and the coping mechanisms they adopt to reduce uncertainty. Peruvians need elaborate legal systems to provide structure to their daily life. Yet, Peruvians deal with uncertainty by transgressing the law (Hofstede, 2001). Thus, if the same applies to organizational context, it is possible that the coping mechanisms defined by PMT would not apply in Peru. That is, PMT assumes that to reduce potential threat, individuals will avoid or reduce maladaptive behavior (Maddux & Rogers, 1983). However, in cultures where people are used to circumvent the law, avoiding risk may not necessarily result in reduced risky behavior.

2.2.2. *Perceived threat*

Security threats reflect a broad range of forces capable of inducing adverse consequences (Loch, Carr, & Warkentin, 1992). Witte (1992) defined a threat as an external stimulus that exists whether or not it is perceived by an individual. Threats may be dynamic and vary over time to adjust to various deterrent and preventive efforts (Schuessler, 2009; Yeh & Chang, 2007). For example, Yeh and Chang (2007) conducted an empirical study of 109 Taiwanese firms. They found that a threat through the network was rated as the most severe threat, but showed the lowest level of protection. IS security threats such as access to systems by competitors, interruptions, interception, modifications, and fabrication can force organizations to pursue more enhanced IS security models, and develop security strategies and policies (Yeh & Chang, 2007).

Previous studies differentiate two kinds of threats (Johnston & Warkentin, 2010; Rogers, 1975; Witte, 1992; Witte, Cameron, McKeon, & Berkowitz, 1996). Perceived threat severity refers to the establishment of a belief reflecting the seriousness of the threat, the probability of personally experiencing the threat, and the ability to enact anti-spyware protection. Perceived threat susceptibility refers to the end-user's perception of the probability of encountering a threat. Appendix 1 summarizes the aforementioned studies. Figure 1 describes the conceptual model used in this study.

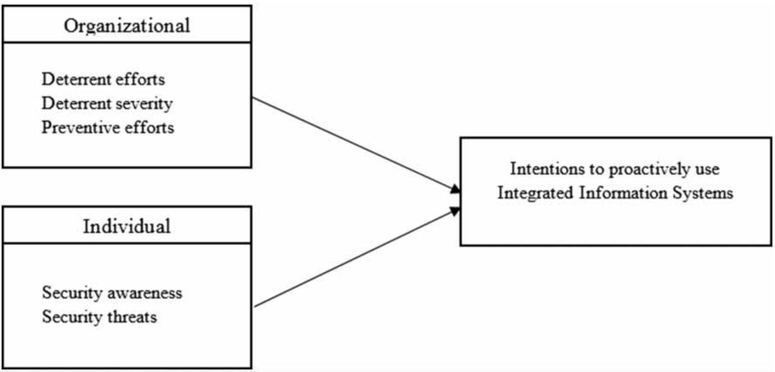


Figure 1. Conceptual model.

3. The case of the Peruvian web-based IIS

CEPLAN (National Center for Strategic Planning: Centro Nacional de Planeamiento Estratégico) is an agency attached to the Peruvian Presidency of Council of Ministers and is responsible for formulating and executing strategic plans for the harmonious and sustainable development of the country, and for strengthening democratic governance (CEPLAN, 2010). CEPLAN is instructed to gather and share information from SINAPLAN (National Systems of Strategic Planning: Sistema Nacional de Planeamiento Estratégico) entities. These entities are public-sector organizations such as the national, regional, and local government agencies. To achieve their goal, CEPLAN has been developing a Web-based e-government system. The system has to integrate information from the various systems currently deployed by SINAPLAN. Figure 2 shows the architecture of the system (thereafter, IIS).

The IIS consists of four core components: Module Information for Strategic Planning (MIPE), Integrated Monitoring and Evaluation (SIME), National Systems of Plans (SINPLE), and Bank of Programs and Strategic Projects (BANPPLE) as described in Table 1. Three departments of CEPLAN including DNSE (National Office of Monitoring and Evaluation), DNPE (National Office of Forecasting and Strategic Studies), and DNCP (National Office of Coordinating and strategic Planning) play important roles in developing and managing the Web-based IIS.

The Web-based IIS implementation was conducted in three phases. The first phase included the implementation and testing of the pilot. Five percent of the SINAPLAN entities were expected to adopt the system during the pilot testing. The first phase also included training and the completion of the conceptual design of the system. In the second phase of the roll-out, approximately 30% of the entities were expected to use the system. In the final phase, up to 65% of the SINAPLAN entities were expected to use the system. Although the adoption of the system was detailed in a government directive,[2] users' resistance could hinder post-adoption use and the subsequent success of the IIS. Thus, as part of the pilot, the Peruvian government was

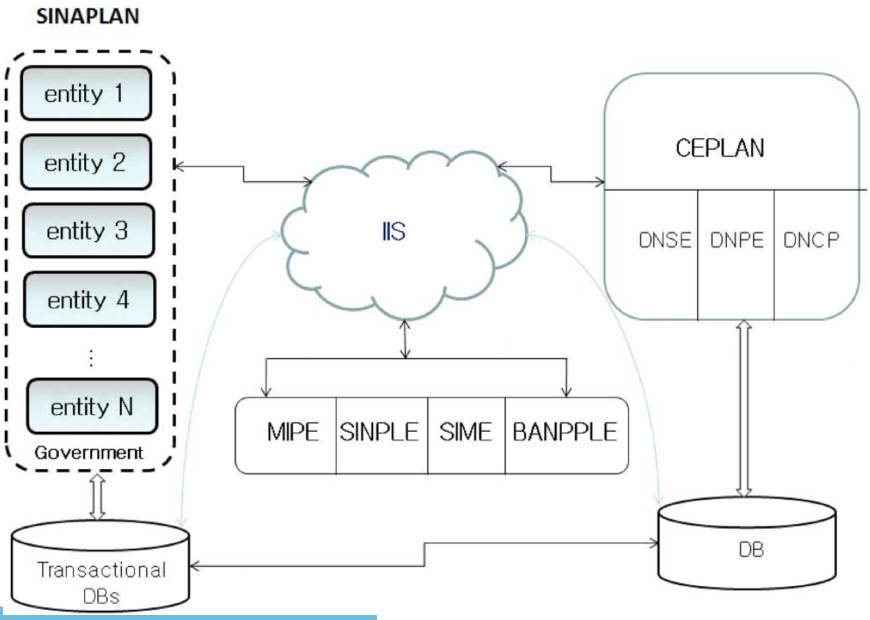


Figure 2. Web-based IIS for CEPLAN in Peru (adapted from CEPLAN, 2010).

Table 1. An overview of the four modules.

Modules	Overview
MIPE (Module Information for Strategic Planning: Modulo de Información para el Planeamiento Estratégico)	Collecting data from SINAPLAN entities and distributing guidelines and policies about strategic plans
SINPLE (National System of Plans: Sistema Nacional de Planes Estratégicos)	Supporting enrollment of strategic plans being formulated by SINAPLAN entities
SIME (Integrated Monitoring and Evaluation: Sistema de Monitoreo y Evaluación)	Monitoring and evaluating strategic plans
BANPPE (Bank of Programs and Strategic Projects: Banco de Programas y Proyectos Estratégicos)	Serving as a repository of various programs, strategic projects, and strategic development plans, among others

Source: Adapted from CEPLAN (2010).

interested in assessing factors that might influence users' attitude towards the system. Research on users' acceptance and usage behavior suggest that users' beliefs and attitude drive IT usage (Bhattacherjee & Premkumar, 2004). Understanding users' perceptions and attitude at the post-adoption stage can provide insights to the effective utilization of the IIS after the initial adoption (Saeed & Abdinnour-Helm, 2008). Since the study was conducted during the first phase of the implementation, the dependent variable measured "intention to use" and not "actual use."

4. Research model and hypotheses

Out study set to investigate the information security factors that influence intentions to use a Web-based IIS in Peru. Prior studies traditionally focused on organizational level security (i.e. Straub, 1990) or on misuse at the individual level (D'Arcy et al., 2009; Hovav & D'Arcy, 2012). In this study, we examine both organizational and individual information security factors.

Although the use of the IIS is not voluntary for SINAPLAN entities, it is important to investigate its use intentions because users' resistance can hinder the success of a system. In particular, as the IIS is subject to the step-by-step implementation as described in the previous section, it is necessary to identify users' intentions to use the system at its conceptual design or initial development stages. Intention affects an individual actual behavior. The degree and speed of the successful diffusion of an innovation or policy depends on users' intention even when the implemented system is mandatory.

4.1. *Organizational factors*

Deterrent efforts directly influence the probability that IS security abusers will be caught (Kankanhalli et al., 2003). Deterrent efforts measured in man-hours spent on security-related efforts were also found to result in better IS security effectiveness (Kankanhalli et al., 2003). The intention to use a new system may be hindered by users' perceptions of risk (Aladwani, 2001). In our case, these risks may involve substantial loss through unauthorized disclosure, and the modification or destruction of information. Although these issues are universal, they are augmented by the conditions in Peru (UN, 2012). First, the lack of technical capabilities is likely to constraint the implementation of an e-government (Belanger & Hiller, 2006). From an information security perspective, the relatively underdeveloped infrastructure available in Peru prevents the implementation of advance security software, increasing perceptions of risk. Second, low cyber security skills increase misuse intentions (Choi, Levy, & Hovav, 2013). Peru's ICT index, and subsequently, the number of computer savvy users are also relatively low. Finally, the relatively high levels of corruption and the fact that the system is managed by a third-party vendor provide government entities with minimal control over the system and its security. Therefore, we posit that when government users perceive a lower cyber security risk due to increasing deterrent efforts, their intentions to use the IIS are likely to increase. Since we measure deterrence efforts as the number of employees working in information security-related capacity and the total number of hours per week spent on information security activities (Kankanhalli et al., 2003), we propose the following hypotheses:

> Hypothesis 1a: There is a positive relationship between the perceived number of employees engaged in information security activities and Peruvian government employees' intentions to use the IIS.
>
> Hypothesis 1b: There is a positive relationship between the perceived total number of hours per week spent on information security activities and Peruvian government employees' intentions to use the IIS.

Deterrent severity refers to the severity of sanctions that dissuade people from IS security abuse by ensuring that they will be severely punished if caught (D'Arcy et al., 2009). Therefore, the existence of a severe punishment system is likely to reduce the number of security incidents an organization will experience. In this study, we measure users' perception of the punishment they are likely to receive if caught misusing information assets as suggested by Kankanhalli et al. (2003). Following the logic used for H1a and H1b, we posit that when users perceive the punishment for system misuse as high, they will have fewer concerns regarding potential security incidents. Thus, their intentions to use the IIS are likely to increase. Hence:

> Hypothesis 2: There is a positive relationship between perceived organizational deterrent severity and Peruvian government employees' intention to use the IIS.

Preventive efforts refer to attempts limiting criminal behavior through controls (Forcht, 1994). In the IS context, these controls refer to a number of advanced security software tools. Computer abuse can be prevented by the use of advanced security software and hardware (Nance & Straub, 1988; Straub, 1990). Preventive efforts can discourage illegitimate activities (Gopal & Sanders, 1997). More advanced security software tends to provide more sophisticated access control, thereby making it more difficult for people to engage in IS abuse (Kankanhalli et al., 2003). In addition, monitoring systems can detect unauthorized IS activities through surveillance mechanisms and creation of exception reports (Kankanhalli et al., 2003). Thus, in some cases, monitoring is also likely to reduce misuse intention (D'Arcy et al., 2009). Overall, preventive measures are positively associated with information security effectiveness and decrease potential threat (Schuessler, 2009). Users are more likely to trust a system that has more controls. Such systems are less likely to be abused by intruders. As apparent from Figure 2, the system in question is a complex integrative system to be used by a number of government agencies and local and regional municipalities. Much as cyber security is not limited to sub-organizational boundaries, so are preventive controls. In this study, we measure users' perceptions of the number of software and hardware security solutions used by the organization rather than only the controls used by the IIS. This is because it is difficult to delineate between controls that only protect the system itself and controls that protect the infrastructure used by the system (e.g. firewalls, antivirus software, and intrusion detection software). We therefore hypothesize that:

> Hypothesis 3: There is positive relationship between the perceived number of security solutions the organization introduces as part of its preventive efforts and Peruvian government employees' intention to use the IIS.

4.2. *Individual factors*

User awareness was found to have a strong influence on misuse intention (D'Arcy et al., 2009). In addition, users' information security awareness has been recognized as an important factor in security effectiveness (Cavusoglu et al., 2009; Ku et al., 2009; Rezgui & Marks, 2008; Siponen, 2000; Straub & Welke, 1998). For example, users should be aware of disciplinary actions, risks, and potential losses resulting from noncompliance with organizational information security policies (Barman, 2002; Furnell et al., 1996). Users should be informed through IS security awareness of their role in protecting information assets (Martins & Eloff, 2002).

As mentioned earlier, Peru's ICT index is one of the lowest in South America. The level of computer sophistication in general and security know-how in particular of government employees are also expected to be relatively low. Subsequently, information security awareness may play an even more significant role in setting users' security expectations and behavior. We expect that the more aware users are of the security activities related to the IIS, the more likely they are to use it. Hence:

> Hypothesis 4: There is a positive relationship between the level of Peruvian government employees' information security awareness and the intention to use the IIS.

Industry and academic studies have confirmed that the greatest threats are within the organization (Abu-Musa, 2003; Loch et al., 1992; Ryan & Bordoloi, 1997). Once an individual is conscious of a security threat, he or she will establish beliefs as to the seriousness of the threat and probability of personally experiencing the threat (Johnston & Warkentin, 2010; Vance, Siponen, & Pahnila, 2012). Thus, IIS users should be able to formulate perceived threat severity and perceived threat susceptibility (Witte, 1992; Witte et al., 1996) if they are aware of the existence of that threat.

Several studies have investigated information security threats in different contexts. Spicer (2004) showed that Canadian practitioners perceive a lower threat level than is perceived in other geographic areas. Abu-Musa (2005) study of computer users in Saudi organizations found that almost half of the responding organizations have suffered financial losses due to internal and external threats. He reported that accidental and intentional entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, employees' sharing of passwords, suppression and destruction of output, unauthorized document visibility, and misdirecting prints and distributing information to people not entitled to receive them are the most common security threats to computerized accounting. Yeh and Chang (2007) revealed that managers of highly computerized industries such as the banking and finance sectors have higher levels of perceived threat.

The Fear Appeal Model used by Johnston and Warkentin (2010) showed that fear appeal does impact end user behavioral intentions to comply with recommended acts of security. As safety needs (the desire to feel safe and secure, and free from threats) rank high among our needs (Maslow, 1954), people are likely to sustain a feeling of security through compliance with security procedures (Siponen, 2000). However, Web-based IIS may involve greater risks in comparison to traditional IS since potential users may not fully recognize all possible threats. This lack of awareness is likely to be more salient in Peru as the level of ICT is relatively low. Thus, perceived security threat is likely to have a negative impact on users' intention to adopt and use the proposed IIS. Hence, we postulate that:

> Hypothesis 5: Peruvian Government employees' perceived information security threats have negative effects on intentions to use the IIS.

5. Methodology

Table 2 summarizes the operationalization of the aforementioned constructs. As noted in the table, most constructs were adapted from prior studies. A survey instrument was used to measure the constructs. We measured the organizational factors portion of our survey using Straub (1990) and Kankanhalli et al. (2003) measurements since they measured deterrence and preventive efforts at the organizational level rather than at the individual level (i.e. D'Arcy et al., 2009). Straub (1990) measured deterrent efforts as the number of security staff working in the organization and the number of security hours per week. Deterrent severity was measured by severity of penalties for abuse and preventive efforts were measured by the number of security software packages in use. Kankanhalli et al. (2003) measured deterrent efforts using total man-hours expended on IS security purposes per week. Deterrent severity was assessed based on the most severe form of punishment taken by the organization and preventive efforts were gauged using the level of sophistication of security software used in the organization. On the other hand, the individual factors were measured using Bulgurcu et al. (2010) and Johnston and Warkentin (2010). The security awareness measurements developed by Bulgurcu et al. (2010) have been cited over 200 times. We acknowledge that other measures might have provided us with different results. However, the research design used by others did not match the research design of this study. For example, D'Arcy et al. (2009) and Hovav and D'Arcy (2012) research design was based on scenarios, while Siponen and Vance (2010) and D'Arcy and Devaraj (2012) conducted field experiments. Appendix 2 lists the survey items.

Peru has 1985 SINAPLAN entities that were eligible to use the aforementioned IIS. Majority of these entities are local government agencies. Six hundred SINAPLAN entities were selected

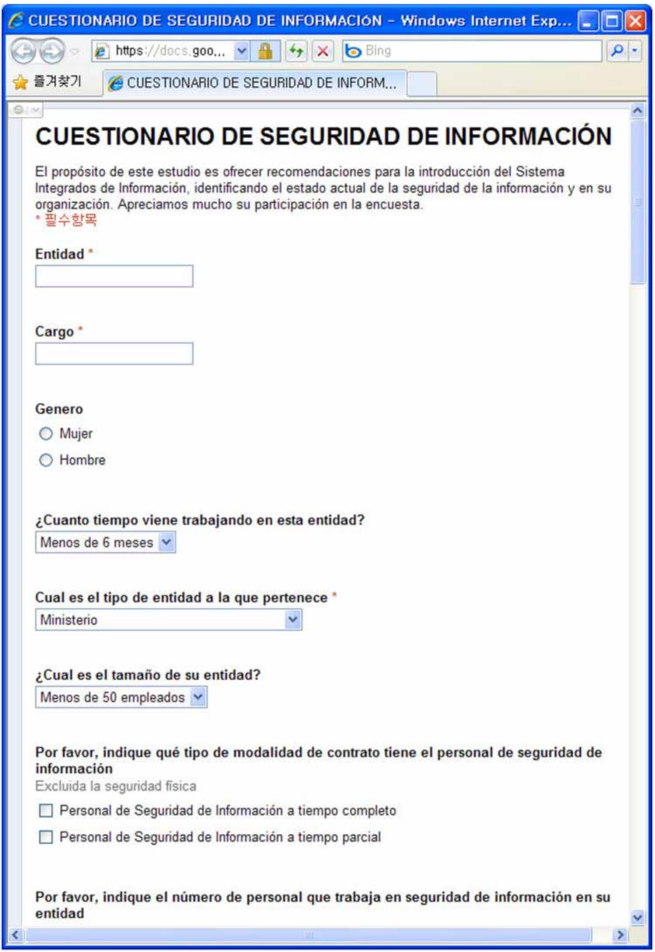
Table 2. Operationalization and measures.

Constructs	Definition	Measures	Sources
Deterrent efforts	Efforts to directly reduce IS security abuse	The number of personnel working in information security activities and the total number of hours per week spent on information security activities	Kankanhalli et al. (2003) Straub (1990)
Deterrent severity	The severity of sanctions dissuading people from IS security abuse	The severity of penalties for employees' noncompliance with information security rules or regulations	Kankanhalli et al. (2003)
Preventive efforts	Efforts to limit illegitimate activities through security solutions	The number of software solutions for information security	Kankanhalli et al. (2003) Straub (1990)
Information security awareness	IS security policy awareness, knowledge and understanding of their responsibilities, negative consequences of noncompliance with information security policy and potential cost	Six items including awareness of general information security and information security policies	Bulgurcu et al. (2010)
Information security threats	Perceived threat severity and susceptibility	Three items including threats to computer viruses, negative consequences, and fear	Johnston and Warkentin (2010)

as a target population for the study. The president of CEPLAN sent formal emails asking for participation in the study. Subsequently, the survey was sent to the managers responsible for the introduction of the IIS in their respective organizations. The questionnaire was written in Google Docs format (Figure 3). One hundred and forty-five usable surveys were completed for a response rate of 24.16%.

Table 3 shows the state of information security of the responding organizations. Seventy seven percent of organizations employ no more than five people dedicated to information security. Thirteen percent of organizations spend more than 16 hours on information security. In all, 6.8% of organizations imposed employment termination as a penalty to employees who did not comply with information security rules or regulations and 7.6% of the organizations take legal action for such behavior. As shown in Table 3, only 1% of the organizations introduced authentication systems based on public key infrastructure.

Each questionnaire item used to measure the three constructs in Table 5 was assessed using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). Following Kankanhalli et al. (2003), we used the number of hours per week spent on information security efforts to measure deterrence efforts. The hours per week spent on information security data was


CUESTIONARIO DE SEGURIDAD DE INFORMACIÓN - Windows Internet Exp...
https://docs.goo...
Bing
즐겨찾기
CUESTIONARIO DE SEGURIDAD DE INFORM...

CUESTIONARIO DE SEGURIDAD DE INFORMACIÓN

El propósito de este estudio es ofrecer recomendaciones para la introducción del Sistema Integrados de Información, identificando el estado actual de la seguridad de la información y en su organización. Apreciamos mucho su participación en la encuesta.
* 필수항목

Entidad *

Cargo *

Genero
○ Mujer
○ Hombre

¿Cuanto tiempo viene trabajando en esta entidad?
Menos de 6 meses

Cual es el tipo de entidad a la que pertenece *
Ministerio

¿Cual es el tamaño de su entidad?
Menos de 50 empleados

Por favor, indique qué tipo de modalidad de contrato tiene el personal de seguridad de información
Excluida la seguridad física
□ Personal de Seguridad de Información a tiempo completo
□ Personal de Seguridad de Información a tiempo parcial

Por favor, indique el número de personal que trabaja en seguridad de información en su entidad

Figure 3. Example of the questionnaire in Google Docs.

Table 3. User organizations: status of information security in SINAPLAN entities.

Information security measures	Type	Number of employees (ratio, %)
Number of employees working in information security	0–10	111 (76.6%)
	11–20	24 (16.6%)
	21–30	8 (5.5%)
	31–40	0 (0.0%)
	41–50	2 (1.4%)
Number of hours per week spent on information security (excluding physical security)	Less than 5 hours	59 (40.7%)
	6–15 hours	38 (26.2%)
	16–25 hours	6 (4.1%)
	26–45 hours	12 (8.3%)
	More than 46 hours	30 (20.7%)
Deterrent severity	No action is taken	12 (8.3%)
	Reprimand by management	30 (20.7%)
	Suspension of duties	82 (56.6%)
	Dismissal from appointment	10 (6.8%)
	Prosecution in court	11 (7.6%)
Preventive efforts	Advanced security software embedded in operating systems	54 (37.2%)
	Advanced security software embedded in database management systems	54 (37.2%)
	Vaccine antivirus	130 (89.7%)
	Firewalls	121(83.4%)
	Intrusion detection systems	89 (61.4%)
	Vulnerability check	48 (33.1%)
	Data loss prevention and backup systems	91 (62.8%)
	Encryption and digital signature systems	32(22.1%)
	Authentication based on public key infrastructure	2(1.4%)

coded as follows. Less than 5 hours was coded as 1, 6–15 hours as 2, 16–25 hours as 3, 26–45 hours as 4, and more than 46 hours as 5. In addition, we measured the number of employees assigned to the security function. The number of employees' data in Table 4 was coded as follow. 0–10 employees were coded as 1, 11–20 employees as 2, 21–30 employees as 3, 31–40 employees as 4, and 41–50 employees as 5.[3] The number of employees and hours spent on information security reflect actual figures obtained by the responding managers from records available to each agency.

The deterrent severity was assessed based on the most severe form of punishment imposed by an organization and was coded as follow (Kankanhalli et al., 2003): no action taken (1), reprimand by management (2), suspension of duties (3), dismissal from appointment (4), and prosecution in court (5). Preventive efforts were gauged by using the number of security software used in the organization. Table 4 shows the number of preventive technologies used in the surveyed organizations and the frequency of each. The average number of security software used is 4.28. None of the organizations had nine security software solutions.

To analyze the model, we ran a multiple regression analysis using SPSS Version 20. Although many contemporary quantitative studies have used Structural Equation Modeling,

Table 4. Preventive efforts distribution.

Number of preventive technologies per organization	Frequency	Percentage
1	13	9.0
2	11	7.6
3	35	24.1
4	24	16.6
5	15	10.3
6	31	21.4
7	4	2.8
8	12	8.3
9	0	0.0

Table 5. Information security awareness, threats, and intention to use IIS.

Dimension (variable)	Mean (standard deviation)	Cronbach alpha	Number of items
Information security awareness	3.07 (0.509)	0.512	6
Information security threats	3.46 (0.901)	0.471	3
Intention to use IIS	4.18 (0.647)	0.412	3

Note: 1: strongly disagree, 3: neutral, 5: strongly agree.

we chose to analyze our model using a regression. Our choice was based on several factors. First, this is an exploratory study. Second, the goal of the study was to examine the relationships between IS security factors and intention to proactively use a Web-based IIS. Thus, the research model does not include mediating variables. Third, multiple regression techniques have been used to test similar research models (e.g. see Lian & Lin, 2008).

A confirmatory analysis of the two reflective independent variables and the dependent variable showed a low convergence. This is despite the fact that the instrument used was identical to questions used in previous studies.

6. Results

As apparent from Table 5, the level of information security awareness was not high (mean = 3.07). However, most interviewees were willing to use the Web-based IIS (mean = 4.18). Table 6 shows the results of the multiple regression analysis between the organizational characteristics and use intentions. In general, collinearity statistics is used to check the independence among the independent variables (Cenfetelli & Bassellier, 2009). Tolerance of less than 0.20 or a

Table 6. Regression analysis between organizational characteristics and use intentions.

Independent variables	Standardized coefficient	*t*-Value (significance level)	Hypothesis result	Tolerance (VIF)
Deterrent efforts: No. of employees	0.013	0.162 (0.872)	Rejected	0.982 (1.018)
Deterrent efforts: No. of hours	0.049	0.565 (0.573)	Rejected	0.979 (1.022)
Deterrent severity	0.113	1.351 (0.179)	Rejected	0.983 (1.017)
Preventive efforts	0.243	2.881 (0.005)	Supported	0.986 (1.015)
Information security awareness	0.164	2.047 (0.042)	Supported	0.997 (1.003)
Information security threats	−0.240	−2.996 (0.003)	Supported	0.997 (1.003)

Variance Inflation Factor (VIF) of 5.0 and above indicates a multicollinearity problem. Both tolerance and VIF values are satisfactory as shown in Table 6. Hypotheses 1a, 1b and 2 were not supported. Hypothesis 3 was supported at $p < 0.01$. Hypothesis 4 was supported at $p < 0.050$ and hypothesis 5 was supported at $p < 0.01$. Thus, preventive efforts and user information security awareness increase SINAPLAN entities intention to use the new IIS while information security threat perceptions have negative influence on intention to use the system.

7. Discussion

As predicted, users' awareness of information security was found to have a positive influence on the intentions to use the IIS. Conversely, users' awareness of potential security threat was found to reduce government entities intentions to use the IIS. Thus, both individual factors were found to have a significant influence on employees' intentions to use the system.

At the organizational level, users perceptions of the level of preventive efforts used were found to increase the intentions to use the system. This suggests that in the context of the Peruvian CEPLAN IIS, the more information security solutions the organization introduces as part of its preventive efforts, the more likely employees are to use the system. It is possible that an excessive use of preventive measures will result in users' resistance as suggested by Youn and Hovav (2013). However, since we did not measure the effect of security overload on IIS use, we cannot comment on the subject.

The remaining three organizational factors were not found to have an impact on intention to use the IIS. Deterrent efforts (number of employees and hours) had no influence on use intentions. It is possible that in bureaucratic countries, where the government employs a large number of workers, the correlation between the size of the workforce and its effectiveness is unclear. Thus, measuring deterrence effectiveness by the amount of resources invested in the information security function might be proper in lean, market driven organizations. Such measures might be misleading in an administrative government organization. Future research can examine the relationships between the actual and the perceived deterrence effort in various types of organizational structures and cultures.

Unexpectedly, deterrent severity had no influence on use intentions. This is surprising considering the fact that 15% of respondents cited dismissal or prosecution as a punishment for non-compliance with security policies. More research is needed to understand the relationships between official punishment measures and actual actions taken. In addition, prior studies found that users do not believe that they or others will get caught when they engage in misuse behavior (D'Arcy et al., 2009). It is possible that respondents stated the official measures as requested, but did not believe that these measures will deter hackers. This might be even more pronounced in countries where bribes often replace proper execution of the law. Further research is needed to better understand the relationships between official policies and actual organizational interpretation of such policies especially in developing countries. Another potential reason that our findings differ from prior studies is our outcome (dependent variable). While prior studies examined misuse intention, IS abuse or security effectiveness, our study examined the effect of security efforts on the intentions to use a system.

8. Implications for research and practice

This is a preliminary investigation to the influence of cyber security perceptions in the context of an e-government system in South America. Given the limited scope of the project and the poor loading of the constructs, the results should be interpreted with caution. Additionally, the results cannot be generalized beyond the study context.

Our study contributes to the security body of knowledge by investigating the influence of security on the acceptance of a new e-government system in a developing country. From a research perspective, to the best of our knowledge, this is the first study that examined the relationships between perceived system security and intention to use. Prior studies examined misuse intentions with the underlining assumption that perceived security would lead to increase use. Our study examined employees' actual intentions to use a system depending on how secure they believe it to be. To the best of our knowledge, this is also the first study to examine and empirically validate cyber security issues and their influence on intention to use an information system in a developing country with relatively low ICT score. As such, deterrence (i.e. convincing users to comply with security rules) had no influence on intention to use. However, prevention (actually using hardware and software tools to prevent misuse) had an effect. These results align with Hofstede analysis of the Peruvian society attitude towards the legal system as discussed earlier.

From a practical perspective, our results suggest that Peruvian organizations should focus on preventive efforts by introducing various information security solutions and improve information security awareness while reducing perceived information security threats. As companies globalize and move to less developed countries, managers should consider the differential attitudes and perceptions of culturally diverse employees. While some measures might work for one culture, they might not work for another. In a culture such as Peru (and other formally Spanish occupied South American countries), where there is a difference between the legal world (rules and policies) and the real world (peoples' actual actions), organizations have to emphasis prevention rather than deterrence.

In calling attention to the study's limitations, we offer suggestions for future research. The generalizability of the study is limited to a government agency in Peru. Extending this study to other types of organizations, regions, and countries at various levels of development can broaden our understanding of the relationships between perceive security and system usage. Our model measured the direct effect of security on intention to use. However, these relationships may be moderated by factors such as perceive trust, organizational leadership, and incentives. Future research may examine the effect of individual, organizational, and cultural factors on the relationship between perceived security and use intentions. Finally, we conducted the study during the initial stages of the system's roll-out. Overtime, users' attitude may change. A longitudinal study (i.e. a revisit of the project) may shed light on the attitudinal change of users once they become familiar with the system and its security measures.

9. Conclusions

The Web-based IIS for formulating a strategic plan of the Peruvian government is a critical e-government system requiring high levels of information security. Our study set to examine organizational and individual security-related determinants for the use of an e-government Web-based IIS in Peru. Peru is an emerging economy with relatively low ICT index and limited use of e-government. In addition, Peru's high corruption index increases the likelihood that employees will be reluctant to use the system due to possible hacking, information leakage, and privacy issues. The system's implementation was facilitated by KDI and CEPLAN, and is maintained by a private vendor. Therefore, it is likely that the government agencies involved perceive a lack of control over the system and regard it as risky. Our findings provide evidence of the significant impact of organizational (e.g. preventive efforts) and individual (e.g. security awareness and threats) factors on the use intention of a Peruvian web-based IIS. Akin to Kankanhalli et al. (2003) findings, deterrence severity had no influence on usage intentions, while preventive efforts did. However, contrary to prior studies (Straub, 1990; Kankanhalli et al., 2003; Whitman, 2004), we did not find deterrence efforts at the organizational level to significantly influence users perception of IS security effectiveness to the extent that it influences proactive use of the system. Thus, while traditional deterrence theory, founded in criminology, assumes that perceive certainty and severity of punishment weigh equally on persons' compliance with the law (Gibbs, 1975), research in the context of information security have found differential influence of deterrence on users' perceptions and behavior. These findings suggest that deterrent efforts and deterrent severity are not motivators but hygiene factors based on the two-factor theory (Hertzberg, Mausner, & Synderman, 1959). According to Hertzberg's two-factor theory (Hertzberg et al., 1959), motivation factors are satisfiers driving an employee's satisfaction, whereas hygiene factors are dissatisfiers affecting an employee's dissatisfaction although they have no influence on satisfaction. Swan and Combs (1976) have used the two-factor theory to explain consumer satisfaction in the context of marketing, where expressive variables as motivators refer to user's psychological level of performance responding to an item of clothing, while instrumental variables as hygiene factors correspond to the performance of the physical product per se. Lee, Shin, and Lee (2007) applied the two-factor theory to usage of mobile data services at the post-adoption stage. According to Lee et al. (2007), information quality as a satisfier increases customers' motivation for mobile service usage, whereas inadequate system quality as a dissatisfier decreases mobile service usage. In other words, system quality has no positive influence on mobile data service usage. Based on the earlier discussion, we maintain that deterrent efforts and deterrent severity play a role of hygiene factors. Additional research is needed to further explore our assertion.

The discrepancy between our findings and prior research may be also due to our target sample. For example, Kankanhalli et al. (2003) surveyed IS managers, while in our study we surveyed casual users. It is very possible that non-IS specialists find it difficult to quantify and ascertain the relationships between deterrence efforts and security effectiveness. Alternatively, our findings may be explained by Yeh and Chang (2007) assertion that there is a gap between managers' security threat perceptions and the actual security countermeasures adopted by the organization. This gap also aligns with the Peruvian society's delineation between the legal and the real.

At the individual level, our findings suggest that users' awareness increases system use intentions while perceive threat reduces intentions to proactively use the IIS. These findings cannot be compared directly with prior studies at the individual level since prior studies use misuse behavior (e.g. D'Arcy et al., 2009; Hovav & D'Arcy, 2012) or compliance behavior (e.g. Bulgurcu et al., 2012; Johnston & Warkentin, 2010) as their dependent variable. However, we are able to compare the levels of awareness in the various populations studied. Users' awareness of security efforts was found to be significantly higher ($p < 0.05$) in the USA than in South Korea with mean = 4.81 and 4.63, respectively (Hovav & D'Arcy, 2012). The awareness level in Peru is even lower (adjusted mean = 4.28). These findings suggest that Peruvian companies and government agencies should improve their security training and educational efforts. Conversely, the perceived threat measured by Johnston and Warkentin (2010) (mean = 3.597) was only slightly higher than that found in our study (mean = 3.46). Incidentally, a study conducted in Indonesia (Putri & Hovav, 2014) found similar results (adjusted mean = 3.64). Thus, we might conclude that security threat perceptions are consistent across countries.

Finally, our findings are partially comparable to Smith and Jamieson (2006) ranking of the drivers of information security perceptions in the context of e-government. Protection of information assets (i.e. preventive measures) was ranked 3rd as a driver. User awareness was found to be a driver (ranked 5th) and lack of awareness an inhibitor (ranked 5th). Conversely, threat perception was not listed as an inhibitor by Smith and Jamieson (2006).

Several studies suggest that trust and reduced risk are likely to increase the use of e-government systems by external users. Our findings suggest that certain preventive (i.e. efforts) and deterrence mechanisms (i.e. awareness) are likely to increase proactive use of e-government IIS, while perceived threat is likely to hinder use intentions.

Funding

This work was partially supported by knowledge sharing programs sponsored by the Ministry of Strategy and Planning in South Korea

Notes

1. http://www.heritage.org/index/country/peru
2. National Strategic Planning Centre (2010), Bicentenary plan: Peru in 2021.
3. None of the entities had more than 50 persons working in information security.

Notes on contributors

Jaehun Joo is a professor of School of Management at Dongguk University, Gyeongju in Korea. His areas of research interest are electronic commerce, information security, business ecosystems, collective intelligence, semantic web, and knowledge management. He has published papers in *International Journal of Human–Computer Studies*, *Journal of Sustainable Tourism*, *Service Business*, *Information Systems Management*, *Expert Systems with Applications*, *Journal of Computer Information Systems*, and *Decision Support Systems*.

Anat Hovav is a professor at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, innovation management, and Futures research. She has published in internationally refereed journals such as *Information Systems Research* (*ISR*), *Information & Management*, *Communications of the ACM*, *Journal of Business Ethics*, *Research Policy*, *Computers & Security*, *Information Systems Journal* (*ISJ*), *Information Systems Management* (*ISM*), *Communications of AIS* (*CAIS*), *Information Systems Frontiers*, and *Risk Management and Insurance Review*. She is the winner of the 2013 citation of excellence award. She has presented her work internationally in academic and industry conferences and workshops.

References

Abu-Musa, A. A. (2003). The perceived threats to the security of computerized accounting information systems. *The Journal of American Academy of Business*, *3*(1), 9–20.

Abu-Musa, A. A. (2005). Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations. *Journal of King Saud University – Computer and Information Sciences*, *18*, 1–26.

Aladwani, A. M. (2001). Change management strategies for successful ERP implementation. *Business Process Management Journal*, *7*(3), 266–275.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: Privacy implications. *Business Process Management Journal*, *12*(1), 48–60.

Barman, S. (2002). *Writing IS security policies*. Indianapolis, IN: New Riders Publishing.

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). On risk, convenience, and Internet shopping behavior. *Communications of the ACM*, *43*(11), 98–105.

Bhattacherjee, A., & Premkumar, G. (2004). Understanding changes in beliefs and attitude towards information technology usage: A theoretical model and longitudinal test. *MIS Quarterly*, *28*(2), 229–254.

Blumstein, A. (1978). *Introduction in deterrence and incapacitation*: *Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

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

Carstensen, P. H., & Vogelsang, L. (2001, June 27–29). *Design of web-based information systems – New challenges for systems development*? Proceedings of the ninth European conference on information systems, Bled, Slovenia.

Cavusoglu, H., Son, J., & Benbasat, I. (2009). *Information security control resources in organizations*: *A multidimensional view and their key drivers* (Working Paper). Vancouver: Sauder School of Business, University of British Columbia.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly*, *33*(4), 689–707.

CEPLAN. (2010). *KSP mission to CEPLAN Peru*. Lima: Author.

Choi, M.-S., Levy, Y., & Hovav, A. (2013, December 14). *The role of users computer self-efficacy, cyber security counter measures awareness and cyber security skills influence on computer misuse*. Proceedings of the pre-ICIS workshop on information security and privacy (WISP2013), Milan, Italy.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98.

Forcht, K. A. (1994). *Computer security management*. Danvers, MA: Boyd & Fraser.

Furnell, S. M., Gaunt, P. N., Holben, R. F., Sanders, P. W., Stockel, C. T., & Warren, M. J. (1996). Assessing staff attitudes towards information security in a European healthcare establishment. *Medical Informatics*, *21*(2), 105–112.

Gibbs, J. P. (1975). *Crime, punishment and deterrence*. New York: Elsevier.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*(4), 29–47.

Hartono, E., Holsapple, C. W., Kim, K.-Y., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, *62*(June), 11–21.

Hertzberg, F., Mausner, B., & Synderman, B. (1959). *The motivation to work* (2nd ed.). New York: Wiley.

Hofstede, G. (2001). *Culture's consequences: Comparing values behaviors, institutions, and organizations across nations*. Thousand Oaks, CA: Sage Publications.

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

Hovland, C., Janis, I. L., & Kelly, H. (1953). *Communication and persuasion*. New Haven, CT: Yale University Press.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory Princely. *Computers & Security*, *31*, 83–95.

Johnston, A. C., & Warkentin, N. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*, 139–154.

Khan, A. R., & Qureshi, M. S. (2009). Web-based information system for blood donation. *Digital Content Technology and its Applications*, *3*(2), 137–142.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers and Security*, *28*(7), 493–508.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security*, *27*, 224–231.

Ku, C. Y., Chang, Y. W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, *33*, 371–384.

Lee, A., & Levy, Y. (2014). The effect of information quality on trust in e-government systems' transformation. *Transforming Government*: *People, Process and Policy*, *8*(1), 76–100.

Lee, S., Shin, B., & Lee, H. (2007). Understanding post-adoption usage of mobile data services: The role of supplier-side variables. *Journal of the Association for Information Systems*, *10*(12), 860–888.

Lian, J. W., & Lin, T. M. (2008). Effects of consumer characteristics on their acceptance of online shopping: Comparisons among different product types. *Computers in Human Behavior*, *24*, 48–65.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, *16*(2), 173–186.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*, 469–479.

Martins, A., & Eloff, J. H. P. (2002, June 25–28). *IS security culture*. Proceedings of IFIP TC-11 17th international conference on IS security, Netherlands.

Maslow, A. H. (1954). *Motivation and personality*. New York: Harper & Row.

Nance, W. D., & Straub, D. W. (1988, November 30–December 3). *An investigation into the use and usefulness of security software in detecting computer abuse*. Proceedings of the ninth annual conference on information systems, Minneapolis, MN, USA.

Pearson, F. S., & Weiner, N. A. (1985). Toward an integration of criminological theories. *Journal of Crime and Criminology*, *76*(1), 116–150.

Putri, F., & Hovav, A. (2014, June 9–11). *Employee compliance with BYOD security policy*: *Insights from reactance, organizational justice, and protection motivation theory*. Proceedings of the 22nd European conference on information systems (ECIS), Tel-Aviv, Israel.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*, 241–253.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 93–114.

Ryan, S. D., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. *Information & Management*, *32*(3), 137–146.

Saeed, K. A., & Abdinnour-Helm, S. (2008). Examining the effects of information system characteristics and perceived usefulness on post adoption usage of information systems. *Information & Management*, *45*(3), 376–386.

Schuessler, J. H. (2009). *General deterrence theory*: *Assessing information systems security effectiveness in large versus small businesses.* Unpublished manuscript, University of North Texas.

Siponen, M., & Vance, A. O. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterl*y, *34*(3), 487–502.

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

Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information system security. *Information Systems Management*, *23*(2), 21–32.

Spicer, G. D. (2004). *Information systems management maturity and information technology security effectiveness*. Unpublished manuscript, University of Lethbridge, Alberta, Canada.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45–62.

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

Swan, J. E., & Combs, L. J. (1976). Product performance and consumer satisfaction: A new concept. *Journal of Marketing*, *40*(2), 25–33.

UN. (2012). *United Nations e-government survey 2012*. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198.

Wangwe, C. K., Eloff, M. M., & Venter, L. (2012). A sustainable information security framework for e-government – Case of Tanzania. *Technological and Economic Development of Economy*, *18*(1), 117–131.

Weber, R. (1988). *EDP auditing*: *Conceptual foundations and practice*. New York: McGraw Hill.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43–57.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society*, *20*(4), 545–572.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monograph*, *59*, 329–349.

Witte, K., Cameron, K. A., McKeon, J. M., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*, 317–342.

Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. *Government Information Quarterly*, *31*(1), 150–159.

Yao, J. T. (2008). An introduction to web-based support systems. *Intelligent Systems*, *17*(1–3), 267–281.

Yeh, Q. Y., & Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information and Management*, *44*(5), 480–491.

Youn, J., & Hovav, A. (2013, April 10–12). *What shapes information system misuse intention? The hidden role of leadership style and perceived organizational justice*. Proceedings of the 12th annual security conference, Las Vegas, NV.

Zhao, J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, 27, 49–56.

Appendix 1. Definitions and previous studies

Focus	Definition	Previous studies
Deterrent efforts	Attempts to discourage deliberate attacks against a system through the dissemination of information and a threat of sanctions in the form of penalties for violation of security policies and security awareness training. These efforts focused on reducing IS abuse and increasing the probability that IS abusers will be caught.	D'Arcy et al. (2009) Kankanhalli et al. (2003) Ku et al. (2009) Spicer (2004) Straub and Nance (1990) Straub (1990) Whitman (2004) Yeh and Chang (2007)
Deterrent severity	The severity of sanctions which can dissuade people from IS security abuse. When caught, abusers severely punished, including reprimands by management, the suspension of duties, dismissals, and prosecution in court.	Bulgurcu et al. (2010) D'Arcy et al. (2009) Kankanhalli et al. (2003) Straub (1990) Whitman (2004)
Preventive efforts	Efforts warding off illegitimate activities through more advanced security software and sophisticated access control that prevent unauthorized access and limit IS abuse.	Gopal and Sanders (1997) Kankanhalli et al. (2003) Nance and Straub (1988) Shuessler (2009) Straub (1990)
Security awareness	Employees' awareness of information security policies and understanding of their responsibilities and negative consequences of noncompliance with information security policies and potential costs.	Bulgurcu et al. (2010) Cavusoglu et al. (2009) D'Arcy et al. (2009) Kritzinger and Smith (2008) Ku et al. (2009)
Security threat	External stimuli that exist regardless of whether they are perceived by an individual, including their perception and fear of the severity of the threat.	Johnston and Warkentin (2010) Witte et al. (1996) Yeh and Chang (2007)

Appendix 2. Information security questionnaire

The purpose of this survey is to offer recommendations for introducing integrated information systems by identifying current status of information security in your organization. We highly appreciate your participation in the survey.

Please read the following questions carefully and indicate your answer with √.

SECTION I.

1	Gender	[ ]Male[ ]Female
2	How long have you been working for your organization?	[ ]less than 6 months[ ]6 months - 1 year[ ]1 - 2 years
		[ ]3-4 years[ ]5-6 years[ ]More than 7 years
3	What type of organization do you work for?	[ ]Ministry[ ]Public Entity[ ]Autonomous Constitutional Body
		[ ]Regional Government[ ]Local Government[ ]Provincial District Municipality
		[ ]Congress[ ]Judicial[ ]Others

SECTION II.

	DETERRENT EFFORT	
4	Please indicate the number of staff working in information security (excluding physical security) in your organization.	[ ]0–5
		[ ]6–10
		[ ]11–20
		[ ]21–50
		[ ]above 50
5	Please indicate how many hours expended for information security purposes per week in your organization.	[ ]16–25 hours
		[ ]26–35 hours
		[ ]36–45 hours
		[ ]More than 46 hours
		[ ]36–45 hours
		[ ]More than 46 hours
	DETERRENT SEVERITY	
6	Please specify what kind of punishment measures are conducted in your organization for noncompliance with information security policy regulations.	[ ]No actions are taken
		[ ]Reprimand by management
		[ ]Suspension of duties
		[ ]Dismissal from appointment
		[ ]Prosecution in court
	PREVENTIVE EFFORTS	
7	Indicate information security prevention systems adopted in your organization (please check as many as possible).	[ ]Advanced security software embedded in Operating Systems
		[ ]Advanced security software embedded in Database Management Systems
		[ ]Vaccine antivirus
		[ ]Firewalls
		[ ]Intrusion detection systems
		[ ]Vulnerability check
		[ ]Data loss prevention and Backup systems
		[ ]Encryption and Digital Signature systems
		[ ]Authentication based on the public key infrastructure

(*Continued*)

Appendix 2. Continued

SECTION III.

SECURITY AWARENESS

8 *Please indicate a single score where 1 represents Strongly Disagree and 5 represents Strongly Agree for each statement.*

STATEMENT	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
A I have sufficient knowledge and understanding regarding Information Security.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
B I have sufficient knowledge of the potential cost of information security problems and threats.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
C I fully understand the concerns about information security and its potential risks.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
D I know and understand all the regulations prescribed by my organization's information security policy.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
E I know my responsibility to improve information security as prescribed by my organization.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
F I have full knowledge of my responsibilities and the cost of noncompliance with my organization's information security.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5

SECURITY THREATS

9 *Please indicate a single score where 1 represents Strongly Disagree and 5 represents Strongly Agree for each statement.*

STATEMENT	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
A It is likely that my computer will become infected with some virus (e.g. malwares, spyware, adware, worms, Trojan horses).	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5

(*Continued*)

Appendix 2. Continued

B If my computer becomes infected by a virus, my organization will face dire consequences.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
C I am afraid of various information security threats under an open network environment like the Internet.	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5

SECTION IV.

INTENTION TO ADOPT SII

CEPLAN designs and implements Web-based information systems (SII: *Sistema de Informacion Integrado*) that integrate all data and information relevant to strategic planning, monitoring and evaluating of strategic management of the state for economic and social development under Plan Peru 2021.

10 *Please indicate a single score where 1 represents Strongly Disagree and 5 represents Strongly Agree with statement.*

STATEMENT	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
A I intend to use Web-based integrated information systems (IIS).	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
B I predict that I will be using Web-based integrated information systems (IIS).	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5
C I plan to use Web-based integrated information systems (IIS).	[ ] 1	[ ] 2	[ ] 3	[ ] 4	[ ] 5