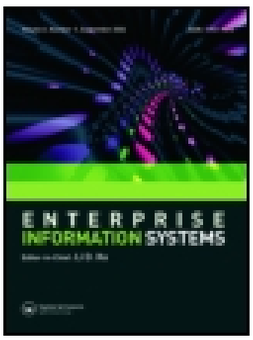

Enterprise Information Systems

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/teis20

Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value

Jiunn-Woei Lian

To cite this article: Jiunn-Woei Lian (2020): Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value, Enterprise Information Systems, DOI: 10.1080/17517575.2020.1791966

To link to this article: https://doi.org/10.1080/17517575.2020.1791966

ENTERPRISE INFORMATION SYSTEMS
https://doi.org/10.1080/17517575.2020.1791966

Taylor & Francis
Taylor & Francis Group

Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value

Jiunn-Woei Lian

Department of Information Management, National Taichung University of Science and Technology, Taichung, Taiwan

ABSTRACT

This research aims at investigating the critical factors that promote users in protecting the Bring Your Own Device (BYOD) information security. Perceived value serves as the core variable and integrates the Technology Threat Avoidance Theory and the Value-based Adoption Model to propose an integrated model. The questionnaire survey employed to verify the hypotheses. The results show that perceived usefulness (positive), perceived threats (positive), perceived expense (negative), impact on systems performance (negative), and user self-efficacy (positive) are the critical factors. The explanatory power (R^2) is 51%. Besides, BYOD security awareness and perceived values affect the intention of BYOD security protection (R^2=62%).

ARTICLE HISTORY
Received 21 January 2020
Accepted 1 July 2020

KEYWORDS
Smart business; bring your own device (BYOD); smart device; information security management; perceived value

1. Introduction

It is known that the Information System (IS) with big data makes business 'smarter' than before. In the manufacturing industry, it makes smart manufacturing, or smart factory in the new era. Also, in the retail industry, it makes smart retailing. Furthermore, in industries like hospitals and education, it makes smart precision hospital and smart precision education, respectively. However, another critical issue, especially in the era of smart devices is how to protect business information security. When this issue occurs in business, it is usually called Bring Your Own Device (BYOD). The increase in the use of cloud computing and smart devices promotes the development of BYOD (Olalere et al. 2015; Baillette, Barlette, and Leclercq-Vandelannoitte 2018) in the workplace. According to the International Data Corporation (IDC), the increase in the use of mobile devices and its upgrade brings new security challenges, promote the awareness of risk management issues, and encourages investment in security technology. From the top 10 IDC 2020 predictions, there was great emphasis on the critical role of the Chief Trust Officer responsible for business security (Gens et al. 2019).

Apart from the traditional IS environment (personal computer-based) with BYOD, cloud computing, and high bandwidth mobile broadband, BYOD allows users to access

CONTACT Jiunn-Woei Lian jwlian@nutc.edu.tw; allenlian@gmail.com Department of Information Management, National Taichung University of Science and Technology, Taichung 40401, Taiwan

big data across different places and times. Of course, the risk is higher than the traditional business IS environment (Agrawal and Tapaswi 2019). For example, in 2020, due to the outbreak of COVID-19, most businesses and schools encourage stay at home for working and learning. Zoom becomes an important tool for online conferencing and learning. Meanwhile, the security challenge of zoom is a typical example of cloud-based BYOD security protection. Hence, there is a high need for novel methods from technical and managerial perspectives. BYOD blurs the difference between the corporate and personal equipment. Imposing new challenges in securing and managing information is good for work as well as personal use (Morrow 2012). Research shows that it involves high-security risk in business and the adoption logic is different from traditional information technology adoption (Baillette, Barlette, and Leclercq-Vandelannoitte 2018). Most of the previous studies stated that the technical and managerial perspectives were relatively fewer. This is one of the gaps in this research area and has become the first motivation of this study.

This study was conducted in Taiwan, a country with SMEs based on the economic system. More than 98% of businesses in Taiwan are SMEs. The fact remains that most large organisations have well-defined BYOD information security policies but security is not always a priority for SMEs (ZyXEL 2015). The major challenge for SMEs in Taiwan as well as some other countries (with SMEs based economic system) is how to balance the business growth and information security. Consequently, we obtain the second motivation of this study.

From the above discussion, this study aimed at investigating and analysing the critical factors that promote users in protecting the BYOD information security in SMEs. This brings us to the following questions:

RQ1. What are the critical factors involved in a user's intention in protecting their BYOD information security spontaneously?

RQ2: What business can be feasible when the intention is relatively low?

2. Literature review

Information security is an interdisciplinary field. Some researchers focused on the technology of information security, while others investigated it by socio-technical methods (Anderson and Agarwal 2010). However, the protection of information security depends on the control and management of technology as well as the management of user's information security behaviour (Ng, Kankanhalli, and Xu 2009)

Few research studies focused on the general user (Anderson and Agarwal 2010). Research shows that BYOD is an issue on both individuals and employees of organisations and there are few references to this issue (Garba et al. 2015). In summary, BYOD information security has become a critical issue in the management of information security in recent years (Putri and Hovav 2014; Garba et al. 2015; Garba, Armarego, and Murray 2015), most especially in the cloud computing environment (Ramachandran 2016).

Kadimo et al. (2018) suggested that device management and data security are the two critical issues relating to BYOD in the medical and health-care industries. Harris, Patten, and Regan (2013) proposed that users of BYOD information security awareness were below the required level. Workman, Bommer, and Straub (2008) presented the idea of a knowing-doing gap, which emphasises on users' inconsistency in knowing the

importance of information security protection, thereby neglecting its implementation. Thus, further investigation is required to disclose its causes.

Regarding the above discussions, this study explores users' behaviour under the circumstances of contemporary trends (cloud computing and BYOD) from a socio-technical perspectives. This section reviews and summarises the previous literature.

2.1 Smart business and information security

The components of smart business are cloud computing, Internet of Things (IoT), big data, and deep learning. Ahmed et al. (2017) studied the role of big data in the IoT applications. However, Zulhuda, Azmi, and Hakiem (2015) and Tarekegn and Munaye (2016) proposed that the Information Technology (IT) applications are not only new technological advancements but there are new concerns with risk, security, and privacy. Kshetri (2013) and Khan et al. (2013) considered the privacy issues regarding cloud service that change the nature of information technology. Ibrahim, Yasemin, and Ozgur (2015) and Olalere et al. (2015) proposed that the security is a critical determinant for organisations integrating smartphones into their internal procedures and operations.

For the smart business environment, the integration of mobile devices and cloud-based applications in the BYOD world is the modern working environment (Steelman, Lacity, and Sabherwal 2016). Mylonas, Kastania, and Gritzalis (2013) proposed that users of smartphones showed security self-satisfaction, which was quite different from their approach to Personal Computers (PCs). Olalere et al. (2015) presented that data leaks, Distributed Denial of Service attacks, and Malware are the most common threats experienced using a BYOD and cloud computing environment. Users excessively trust the platforms from which they download applications. Therefore, they fail to protect their smartphones from common threats (by activating anti-virus software) and ignoring the information security risks during the process of downloading and installation. Corporate managers focused on the security issues of smartphones by considering whether to introduce them into the internal operations or not (Arpaci, Cetin, and Turetken, 2015). Harris, Patten, and Regan (2013) proposed that users lack sufficient information security awareness on BYOD equipment. Further investigation is needed to improve the management of information security of BYOD users and providers (Ramachandran and Chang 2016).

2.2 Information security awareness

Information security awareness is an important factor affecting user behaviours. Few studies were carried out on BYOD users' information security awareness considering the cloud-based environment. This study employs it as BYOD information security awareness and integrates it as part of the research framework.

Information security awareness refers to the idea that users within an organisation should be aware of the need to protect the company's information, usually established through the organisations' information security standards or policies (Siponen 2000). Many organisations wish to promote their employees' information security awareness with various measures, thereby protecting their system security and profits (Kruger and Kearney 2006). Recently, PCs were the primary organisational IT tools used. It was

observed that an organisation could control and manage its information security through an effective auditing mechanism. However, owing to BYOD's increasing popularity, individuals play a critical role in maintaining information security. Sari and Candiwan 2014 presented that employees' lack of information security awareness might become a major threat to an organisation's information security when personal hand-held smartphones became popular.

Previous studies employed various theories to explain the critical factors that have had an impact on employees' awareness and behaviour of information security. Lebek et al. (2013) stated that previous studies on the awareness and behaviour of information security within an organisation were based on the Reasoned Action Theory, Planned Behaviour Theory (PBT), General Deterrence Theory, Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), among others. Bulgurcu, Cavusoglu, and Benbasat (2009) emphasised on employees' information security awareness and the perceived fairness. This had an impact on employees' compliance with the policy of information security. Besides, Huang et al. (2011) discovered that perceived security had an impact on users' intentions and perceived awareness had an impact on perceived security. Rezgui and Marks (2008) aimed their study at the behaviour of school staff in managing information security. They observed that responsibility, culture, religious belief, and social interaction had an impact on employees' information security awareness.

Kruger and Kearney (2006), in their research on the content and measurement of information security awareness, proposed that there are three perspectives of the measurement of information security awareness, namely: knowledge, attitude, and behaviour. Wipawayangkool (2009) investigated the nature of information security awareness and proposed a multi-dimensional theory, dividing information security awareness into two sections, namely: awareness and behaviour. Allam, Flowerday, and Flowerday (2014) discussed employees' information security awareness considering smart devices from three perspectives, namely: knowledge, attitude, and behaviour. In summary, previous studies proposed that they are three dimensions of information security awareness, namely: knowledge, attitude, and behaviour. Based on the aforementioned architecture, Parsons et al. (2014) proposed the Human Aspects of Information Security Questionnaire (HAIS-Q), Sari and Candiwan 2014 applied the Analytic Hierarchy Process to analyse Indonesian users' information security awareness using smartphones. Finally, Mylonas, Kastania, and Gritzalis (2013) conducted a study to investigate users' information security awareness using smartphones.

2.3 Critical factors for users' information security protection behaviour

Considering the investigation of factors in users' information security behaviour, previous studies focused on employees' behaviour. Ng, Kankanhalli, and Xu (2009) proposed that the critical factors in users' information security behaviour include perceived feeling, perceived benefits, self-efficacy, and perceived severity. Rhee, Kim, and Ryu (2009) discovered that the self-efficacy of users' information security protection might be affected by their experience, information security events, general controllability, etc., and their information security protection might be reinforced by excellent self-efficacy of users' information security protection. Furthermore, from the threat and coping appraisal perspectives, Liang and Xue (2010) and Ifinedo (2012) concluded that both perspectives

might have an impact on employees' intention to comply with the information security policy. Ifinedo (2012) applied the PBT and PMT in their study. This study proved that the factors in employees' intention to comply with the information security policy consist of threat appraisal (two variables: perceived vulnerability and perceived severity), coping appraisal (three variables: efficiency, cost, and self-efficacy), attitude, and subjective norm. Siponen (2000) concluded that users' motives and self-choice had an impact on their behaviour, which might affect the information security, including internal motives and external motives. Weeger, Wang, and Gewald (2016) applied the UTAUT theory and recruited students as subjects. They obtained that the expected performance was the key factor for users in accepting BYOD. However, their study revealed that the perceived threat was one of the critical factors for users in accepting BYOD, thereby stressing the importance of users' intention in protecting information security. Finally, Lee et al. (2017) also emphasised the critical role of organisational control towards users BYOD adoption intention.

3. Theoretical background and hypotheses development

This study considers users' intentions in protecting BOYD information security as a process of personal behaviour decisions. Users' perceptions will affect their behaviours towards information security protection (Samonas, Dhillon, and Almusharraf 2020). Therefore, users' evaluation of cost and efficacy determine their security protection behaviour for their IT equipment (BYOD). Both Technology Threat Avoidance (TTAT) and Value-based Adoption Model (VAM) emphasise the decision behaviour model in which users deal with IT applications. This study combines the aforementioned theories to propose an integrated model.

3.1 Technology threat avoidance theory (TTAT)

TTAT is one of the most important theories that explains users' information security behaviour. In 2009, Liang and Xue (2009) proposed an explanatory model for users' avoidance behaviour in handling malicious information technology: TTAT. They believed that avoidance and adoption were two different behaviours. The believed that behaviour models such as TAM were not sufficient to explain users' avoidance behaviour. Therefore, they proposed the TTAT model as a supplementary method. TTAT emphasises the idea that users' avoidance behaviour comes from a decision process of a dynamic positive feedback loop. Users may decide on how to respond to information security threats based on the results of threat appraisal and coping appraisal.

According to these arguments, the TTAT model showed the extent to which perceived susceptibility and perceived severity affect the threats which users perceived. However, personal preference for avoiding risks may have an impact on this evaluation process. Also, perceived effects, cost, and self-efficacy affect perceived avoidability. By the aforementioned appraisals, users could decide their motives and behaviour at which they respond to information security risks. Finally, social influence may affect the threat and coping appraisals. Using PCs, Liang and Xue (2010) conducted an evidence-based study to support their explanatory theory for the intention (56%) and behaviour (21%) of information security protection. Furthermore, Ifinedo's study (2012) was also based on the threat

and coping appraisals. This study employs PBT to investigate the critical factors in employees' intentions to comply with information security policy. Regarding the use of TTAT in understanding BYOD security policy adoption, Cho and Ip (2018) also verified its suitability. Based on the above arguments, this study employs TTAT as a core theory.

3.2 Value-based adoption model (VAM)

Kim, Chan, and Gupta (2007) conducted their research based on maximal economic benefit, rather than investigating IT system users to study the acceptance of information technology (such as research and models based on TAM). They integrated the literature regarding consumers' decision-making into their study to propose VAM, helping to explain the intentions and behaviour of user acceptance of Information Communication Technology (ICT). VAM shows that the benefits and works of ICT have an impact on the perceived value that further affects consumers' intentions. Perceived value plays an intermediate role in this process.

Furthermore, Kim, Chan, and Gupta (2007) investigated how internal and external motives influence the benefit perceptions of IT systems based on the perspective of cognitive evaluation theory. External motives refer to the reward for completing a task (such as a financial incentive). Internal motives focus on the reward for implementing a task (such as a sense of accomplishment). VAM shows that the benefits of motives can positively affect users' perceived value. It further affects their intentions as well as two variables, namely: the perspectives of utilitarianism (usefulness) and the perspectives of hedonism (entertainment).

Alternatively, users' perceived sacrifices that include the idea of cost are financial and non-financial costs. They may affect consumers' perceived value, and consequently, affect users' intentions and behaviour. In VAM, there are basically two variables, namely technicality and perceived expense.

3.3 Research framework and hypotheses development

Figure 1 shows the integrated research model based on VAM. It combines the previous literature regarding the information of security management into an integrated framework. Weeger et al. (2018) proposed a Net-valance model to understand users' intentions towards participation in corporate BYOD programmes. In their model, perceived risk and perceived benefit were two major determinants of users' behavioural intention. In other words, drivers and resistances are the two major dimensions required to understand the perceived value of information security protection in this study. Drivers are made up of perceived usefulness and perceived threats. These may positively affect users' perceived value of BYOD information security protection. Meanwhile, resistances consist of three constructs, namely: perceived cost (direct cost), impact on system performance (indirect cost), and users' perceived barriers. These may negatively affect users' perceived value of BYOD information security protection. The hypotheses are illustrated in the following paragraphs.

In the VAM model, perceived benefits are the critical factor in determining the perceived value. Lebek et al. (2013) investigated employees' BYOD behaviour in organisations and discovered that perceived benefits might positively affect employees'

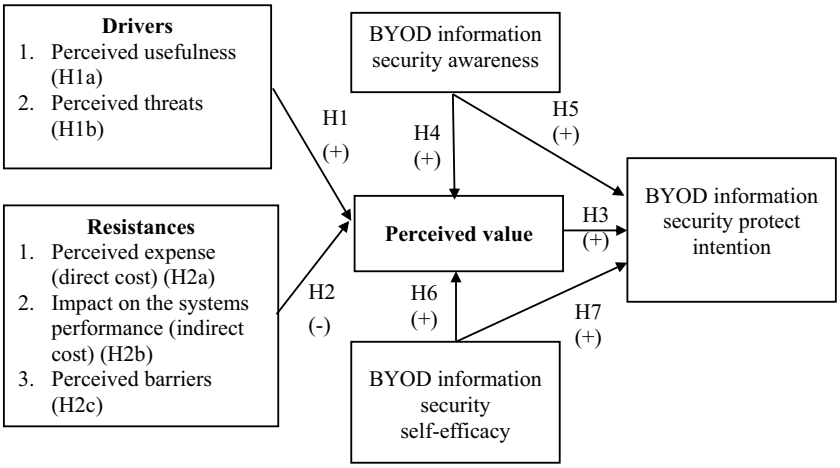

Figure 1. Research model.

intentions to use BYOD. This study employs perceived usefulness as the studied variable which represents perceived benefit (Kim, Chan, and Gupta 2007) and infers Hypothesis 1a.

Yang et al. (2016) discovered the perceived value for a particular information technology determined using the users' perceived benefits and perceived risks. Liu et al. (2015) and Yu et al. (2017) emphasised the impacts of benefits and sacrifices on perceived value for IT applications such as mobile coupons or tablets. Therefore, in addition to the perceived usefulness, users' perceived threats (Anderson and Agarwal 2010) will positively affect their perceived value. Huang et al. (2011) proposed a similar opinion and indicated that perceived risks might have an impact on the intention to comply with information security policy, thereby affecting their behaviour. Based on the arguments, this study infers Hypothesis 1b.

Based on the above discussions, this study categorises perceived benefits (perceived usefulness) and perceived threats as the drivers of positive perceived value. Both are directly proportional to the power of drivers. Therefore, an increase in both lead to an increase in the power of drivers. Hence, this study proposed Hypothesis 1 (H1) and related sub-hypotheses.

H1: The drivers of users' perceived information security protection may positively affect the perceived value of their information security protection.

H1a: The usefulness of users' perceived information security protection may positively affect the perceived value of their information security protection.

H1b: Users' perceived information security threats may positively affect the perceived value of their information security protection.

Regarding the resistances to adopt BYOD information security protection mechanisms, this concept infers from the sacrifices in VAM with traces of other theories entitled as resistances. Three variables included in these categories are perceived expense for

adopting a security protection mechanism, the impact of security protection mechanism on BYOD systems performance, and perceived barrier for installing applications on BYOD.

Perceived cost means the direct cost or the cost of money to instal information security mechanisms. It is the critical factor for determining the perceived value in the VAM model. Liu et al. (2015) emphasised the critical role of cost (perceived financial savings and perceived fees) on the perceived value. TTAT stresses the importance of cost on the management of information security (Liang and Xue 2009). Research publications showed that perceived cost might have an impact on employees' compliance with the BYOD information security policy (Ifinedo 2012; Putri and Hovav 2014). Studies were carried on the negative impact of perceived cost on employees' compliance with information security policy. Consequently, this study proposed that the perceived cost may affect the perceived value and therefore may have an impact on employees' intention to protect information security. Therefore, Hypothesis 2a is proposed.

Direct cost (expense), as well as indirect cost (its influence), are resistance factors considered in this study. Security protection mechanisms increase the system loading an impact on the overall performance. Hayajneh et al. (2013) investigated the impact of the evaluation of information security protection mechanism towards overall network system performance. Besides, TTAT focuses on the effectiveness of information security with coping appraisal. In other words, users can avoid the adoption of information security protection software due to a decrease in system loading and make system operation smoother. Hence, this study employs Hypothesis 2a to emphasise the perceived impact on systems performance.

Finally, users' perceived barriers such as inconvenience, time-consuming, and habit-changing result to user resistance. Ng, Kankanhalli, and Xu (2009) proposed that perceived barriers have negative impacts on users' computer security behaviour. Research showed that there exist perceived barriers for users in adopting an information system based on IS (Granlien and Hertzum 2012). This study holds the perspectives of perceived value, hence perceived value shows the relationship between perceived barriers and proposes the Hypothesis H2 c.

In summary of resistance dimension with three variables, perceived expense (direct cost), impact on system performance (indirect cost), and perceived barriers are the three variables considered in this study. Hence, this proposes Hypothesis 2 (H2) and related sub-hypotheses.

H2: The perceived resistances of users' information security protection mechanism may negatively affect the perceived value of their information security protection mechanism.

H2a: The perceived expense of users' information security protection mechanism may negatively affect the perceived value of their information security protection mechanism.

H2b: The perceived impact of users' information security protection mechanism on system performance may negatively affect the perceived value of their information security protection mechanism.

H2c: The perceived barriers of users' information security protection mechanism may negatively affect the perceived value of their information security protection mechanism.

One of the essential arguments in VAM is that decisions made by consumer cost-benefit analysis may have an impact on the perceived value, thereby affecting its intention (Kim, Chan, and Gupta 2007). Liu et al. (2015) and Yu et al. (2017) investigated and analysed the relationship between the perceived value and behavioural intention. Based on the intention of information security protection, the investigation of H1 and H2 shows that after the decision analysis of benefit and cost, users can evaluate the perceived value of information security protection of BYOD equipment. This aids decision-making when installing an information security protection mechanism on personal equipment. Studies relating to the behaviour of using information systems demonstrated the aforementioned perspectives, that users' perceived value may have an impact on the intention to use information systems or services (Chu and Lu 2007; Wang, Yeh, and Liao 2013; Hsu 2014).

In the perspective of traditional IT adoption in mobile devices or services (BYOD and cloud computing), Kim, Kim, and Wachter (2013) investigated the positive relationships between the perceived value and mobile engagement intention. To understand the drives for purchasing mobile applications, Hsu and Lin (2015) obtained that perceived value is the key determinant of users' purchase intention. Hong, Lin, and Hsieh (2017) proposed the critical determinants of perceived hedonic and utilitarian values to understand users' continuance intention in using a smartwatch.

Therefore, for BYOD information security protection mechanism, we propose Hypothesis 3 (H3) to illustrate the relationship between the perceived value and intention.

H3: The perceived value of BYOD information security protection mechanism may positively affect the intention of information security protection.

Employees' information security awareness is an important factor required to understand users' information security-related issues. Bulgurcu, Cavusoglu, and Benbasat (2010) proposed that it affects employees' beliefs and attitudes towards compliance with information security policy in an organisation. Bauer, and Bernroider (2017) discovered that information security awareness affect user's attitude. In this study, users' beliefs or attitudes relate to their perceived value towards information security protection mechanism.

Ng, Kankanhalli, and Xu (2009) suggested that users' perceived severity determines the strength of the relationship between critical factors and information security behaviour. Perceived severity is attributed to the attitude of information security awareness. Dang-Pham and Pittayachawan (2015) obtained that users' intentions to protect themselves from dangerous software may change according to the perceived vulnerability in the BYOD environment. In other words, the stronger the information security awareness is, the higher the perceived value of BYOD information security protection mechanism will be. This promotes the intention to protect BYOD information security. Consequently, this proposes Hypothesis 4 (H4).

H4: Users' BYOD information security awareness may positively affect users' perceived value of information security protection mechanism.

As discussed in the previous section. Awareness is one of the important issues when considering information security-related issues. Soomro, Shah, and Ahmed (2016)

studied the relationship between BYOD information security awareness and protection intention. They generalised the previous studies and focus on the important role of information security awareness in information security management. They indicated that employees' information security awareness affect their compliance with relative policy and increase their intention to protect information security. Li et al. (2019) emphasised the important role of employees' information security awareness towards their cybersecurity protection intention and behaviour. Although, Bulgurcu, Cavusoglu, and Benbasat (2010) proposed that information security awareness affect users' beliefs and attitudes, and hence influence their intention to comply policy. Also, they investigated the positive relationship between awareness and behavioural intention towards information security protection.

From the aforementioned discussions, we obtained that BYOD information security awareness affect users' perceived value as well as their behavioural intention. Therefore, we have following Hypothesis 5 (H5).

H5: Users' BYOD information security awareness may positively affect users' intentions to protect information security.

Self-efficacy refers to the level of people's confidence in completing specific tasks using their knowledge and skills. It originates from the idea proposed by Bandura (1977) in the theory of social learning. It was applied in learning and later in the investigation of the behaviour of information technology management to understand users' acceptance of information technology. However, self-efficacy was integrated into many kinds of information technology applications, such as self-efficacy on the Internet or electronic commerce. In the area of information security, scholars applied this idea to broaden the understanding of information security management. Rhee, Kim, and Ryu (2009) proposed that self-efficacy in information security enhances users' security practice, strengthens security effort, and security care behaviour.

Vekiri and Chronaki (2008) investigated the effect of self-efficacy on perceived value beliefs of students towards computer use. Thenral and Suganthi (2018) obtained the positive relationship between co-design self-efficacy and perceived value in their study on co-design. In other words, people who have higher self-efficacy will also have higher perceived value. Therefore, in the topic of BYOD information security protection, we deduced that users' information security self-efficacy positively affect their perceived value. Therefore, we obtain Hypothesis 6 (H6).

H6: Users' self-efficacy of BYOD information security may positively affect users' perceived value of BYOD information security protection.

The above discussions about self-efficacy suggest that the relationship between security self-efficacy and security protection intention can be divided into two major topics. Johnston and Warkentin (2010) obtained that system response efficiency, social impact, and self-efficacy were critical factors that affect users' behaviour of information security.

The first one deals with self-efficacy and protecting intention and behaviour. Li et al. (2019), Anderson and Agarwal (2010), Ng, Kankanhalli, and Xu (2009), Rhee, Kim, and Ryu (2009), Johnston and Warkentin (2010) conducted research studies in this area.

Most of these studies indicated that self-efficacy affects users' security protection behaviour in different contexts, such as cyberspace, and workplace. The second aspect deals with information security self-efficacy and policy compliance. Vance, Siponen, and Pahnila (2012) conducted research on employees' compliance with the information security policy of organisations and discovered that employees' self-efficacy may positively affect the intention to comply with the information security policy. Bulgurcu, Cavusoglu, and Benbasat (2010) investigated the positive relationship between self-efficacy and intention to comply with the information security policy. Besides, Ifinedo (2012) conducted a study using PBT and PMT and obtained that employees' self-efficacy may affect their intention to comply with the information security policy.

Finally, a study of BYOD showed that employees' self-efficacy positively affects the intention to protect them from dangerous software (Dang-Pham and Pittayachawan 2015). From the above discussion, we proposes Hypothesis 7 (H7).

H7: Users' self-efficacy of BYOD information security may positively affect the intention to protect the information security.

4. Methodology

In this section, we illustrate the related empirical research designed to verify the proposed hypotheses in the following sub-sections.

4.1 Operational definitions and measurements

Table 1 shows the operational definitions of the aforementioned variables and their measurement methods. This study focuses on SMEs employees, the information security protection means users' adoption of additional mechanisms (such as anti-virus software) on their BYOD devices. Following the above definition, a questionnaire based on the aforementioned measurable parameters was developed. Experts and scholars were invited to review this preliminary version. After drafted, pre-tests were conducted to ensure the reliability and validity of the questionnaire. The students of pre-tests were recruited from college students and master students who use their own devices in the school. The questionnaires were distributed by social media including Facebook and Line. To encourage participation, 15 rewards (convenient store coupons worth of 100 NT Dollars) were provided for the lottery to encourage students to complete the pre-tests. Finally, we collected 116 questionnaires from college students and 23 questionnaires from master students, making a total of 139 pre-tests data. After analysing the results from the pre-tests, we reviewed the questionnaire again to ensure the reliability and validity of the official questionnaire.

4.2 Data collection

This study follows the principle of the Total Design Method (Dillman 1978, 2000). TDM is divided into two levels of investigation. The first level requires the investigation of every

Table 1. Operational definitions and measurements.

Variables	Operational definition	Item number	Sources
Perceived usefulness (PU)	Users' awareness of whether the BYOD information security protection is valid or not.	6	Liang and Xue (2010)
Perceived threats (PT)	Users' awareness of how serious the BYOD information security threats are.	8	Anderson and Agarwal (2010)
Perceived expense (PE)	Perceived expense needed in the BYOD information security protection mechanism.	3	Lin et al. (2012)
Impact on the systems performance (ISP)	Impact on the system performance when information security protection mechanism is installed for BYOD.	3	Workman, Bommer, and Straub (2008)
Perceived barrier (PB)	Perceived barriers for installing information security protection mechanisms on mobile devices.	4	Ng, Kankanhalli, and Xu (2009)
Perceived value (PV)	Users' perceived value of the installed BYOD information security protection mechanism.	4	Kim, Chan, and Gupta (2007)
Self-efficacy (SE)	Users' confidence in being able to protect the information security for BYOD equipment.	11	Rhee, Kim, and Ryu (2009); Liang and Xue (2010)
Information security awareness (ISA)	Users' knowledge, attitude, and behaviour of information security for BYOD equipment.	3	Bulgurcu, Cavusoglu, and Benbasat (2010)
BYOD information security protection intention (ISI)	Users' intentions to protect information security.	4	Rhee, Kim, and Ryu (2009); Liang and Xue (2010)

aspect of a process to ensure that the best results are obtained. The second level requires the integration of all the resources in the study to fulfil its goals. According to the principle of TDM, a recruitment letter was drafted. This is to convince students of the importance of their participation and the mutual benefits to both parties, and to encourage them to complete the questionnaire. To ensure the privacy of participants and the integrity of the research, we conducted this process confidentially.

Furthermore, it focuses on the employees who have smart devices and use them at work, i.e., users of BYOD. Data collection was conducted using an internet-based questionnaire (Google form). The recruitment was conducted through a popular Bulletin Board System (BBS), PTT, which is the largest online forum in Taiwan. We posted the questionnaire on the workplace-related boards. Users who are employees of SMEs were invited to complete the questionnaire. In general, 15 rewards (convenient store coupons worth of 100 NT Dollars) were provided for the lottery to encourage participation. The process of data collection lasted for 10 days (from 3 December 2018 to 13 December 2018) and 309 questionnaires were submitted. Besides 26 questionnaires completed by students (part-time staffs) who did not use personal mobile devices at work, we collected 283 valid questionnaires (participants who had experience of BYOD). Therefore, we had 91.6% valid questionnaires of the total collected questionnaires. We then analyse the data from these 283 valid questionnaires.

5. Results

In this section, we present the distributional structure of samples using descriptive statistics (Table 2). Then, we examine the reliability and validity of the scale (Table 3 and Table 4). We apply the value of Cronbach α to determine the reliability of the scale. And Confirmatory Factor Analysis was applied to test the validity of the scale.

Table 2. Demographics.

Variable		Count (%)
Gender	Male	181 (64%)
	Female	102 (36%)
Age	< 20 years old	7 (2.5%)
	20–25 years old	78 (27.6%)
	26–30 years old	58 (20.5%)
	31–35 years old	70 (24.7%)
	36–40 years old	27 (9.5%)
	41–45 years old	11 (3.9%)
	46–50 years old	2 (0.7%)
	51–55 years old	3 (1.1%)
	56–60 years old	0 (0%)
	61–65 years old	27 (9.5%)
Education	Senior high school and under	27 (9.5%)
	Undergraduate	164 (58%)
	Graduate and higher	92 (32.5%)

Table 3. Validity and reliability.

Variables	CR	AVE	Factor loading	R^2 (Adj-R^2)	Cronbach's α	Item number
Perceived usefulness	0.97	0.84	0.89–0.93	n/a	0.96	6
Perceived threats	0.95	0.70	0.76–0.87	n/a	0.94	8
Perceived expense	0.97	0.90	0.93–0.96	n/a	0.95	3
Impact on the system performance	0.95	0.87	0.93–0.94	n/a	0.93	3
Perceived barrier	0.93	0.77	0.82–0.91	n/a	0.90	4
Perceived value	0.93	0.77	0.84–0.91	0.52 (0.51)	0.90	4
Self-efficacy	0.97	0.76	0.82–0.91	n/a	0.97	11
Information security awareness	0.94	0.83	0.89–0.93	n/a	0.90	3
BYOD information security protect intention	0.90	0.70	0.71–0.91	0.62 (0.62)	0.85	4

Table 4. Discriminant validity.

	Mean	S.D.	PU	PT	PE	ISP	PB	PV	SE	ISA	ISI
PU	5.39	1.10	0.92								
PT	5.83	0.97	0.45	0.84							
PE	4.23	1.39	(0.23)	(0.03)	0.95						
ISP	4.12	1.35	(0.36)	(0.04)	0.55	0.93					
PB	3.69	1.16	(0.36)	(0.07)	0.55	0.75	0.88				
PV	5.06	1.00	0.62	0.41	(0.43)	(0.45)	(0.41)	0.88			
SE	4.94	1.18	0.32	0.22	(0.36)	(0.20)	(0.24)	0.44	0.87		
ISA	5.40	0.99	0.30	0.29	(0.25)	(0.19)	(0.24)	0.40	0.81	0.91	
ISI	5.32	0.91	0.53	0.40	(0.32)	(0.38)	(0.40)	0.65	0.63	0.66	0.84

Except for mean and S.D. of each variable, diagonal value means the square root of AVE for each variable. Other value means the correction coefficients between variables.

Regarding the guidelines presented by Ringle, Sarstedt, and Straub (2012), we employ Partial Least Squares Structural Equation Modelling (Variance-based SEM: PLS-SEM) in hypothesis testing for the following reasons. The major reason is the concern of sample size. Since the respondents who are employees and have cloud-based BYOD experience can participate. Also, there is a need for a willingness to participate. And hence, the sample size is limited. Meanwhile, the covariance-based SEM is sensitive to the sample size (Hair et al. 2014). Besides, the prediction and the high values of the R^2 are important in this study. The PLS-SEM is more suitable in the IS research area. Therefore, we use PLS-SEM to analyse the data instead of covariance-based SEM.

Therefore, smart PLS software was employed to examine the models and hypotheses (Ringle, Wende, and Becker 2015).

Among 283 valid questionnaires, 102 of them were completed by females (36%) and 181 by males (64%). The majority of them were between the ages of 20 years and 35 years (72.8%). We obtained that 18.4%, 14.5%, and 14.1% were from arts/entertainment/leisure, manufacturing, and education, respectively. However, the majority of the participant had an educational background of at least a college qualification (90.5%), a distribution similar to the real workforce in Taiwan. This confirms the representativeness of the data in this study and Table 2 illustrates its details.

Regarding the examination of the reliability and validity of the scale, we apply the following criteria: Composite Reliability value >0.7, Average Variance Extracted (AVE) value >0.5, and Cronbach's α value >0.7. Furthermore, the examination of discriminant validity conducted by comparing them shows that the square root of AVE is larger than the correlation coefficients of variables. All the above criteria satisfy the acceptance range (please see Tables 3 and 4). From the analysis, we have that R^2 of the perceived value is up to 51% and the R^2 of the intention of BYOD information security protection is up to 62%. Therefore, the explanatory variables proposed in this study are with certain R^2.

Furthermore, our results show that the variables that have an impact on users' perceived value of BYOD information security protection mechanism include perceived usefulness (positive), perceived threats (positive), perceived expense (negative), impact on system performance (negative), and users' self-efficacy of BYOD information security (positive). The comprehensive R^2 is up to 51%. For the variables that have an impact on the intention of BYOD information security protection, the R^2 is up to 62%. Such variables are perceived value and users' information security awareness. Table 5 shows the total results of the analysis. The research model for this study has excellent R^2, which can be used as a reference for the academic and business community. The results of hypotheses testing are illustrated in Table 5 and Figure 2.

6. Discussions

This study proposes two research questions in understanding the critical factors involved in a user's intention to protect their BYOD information security and the way to deal with low intention. TTAT (Liang and Xue 2009) and VAM (Kim, Chan, and Gupta 2007) were integrated as the theoretical based in understanding and solving the aforementioned issues.

For the first research question, the study presents the following major findings. Firstly, this study proposes four significant variables regarding the antecedents of perceived value. We obtained that two drivers related variables (perceived usefulness and perceived threats) with significant positive effects. Moreover, two resistances related variables (perceived expense and impact on the performance of the system) have significant negative effects. It was obtained that the perceived barrier which belongs to the resistances, has no significant effect on the perceived value. This means that owing to the increase of information literacy in Taiwan, most of the users are familiar with the use of information applications on their BYOD devices without barriers.

Concerning the second research question, an important determinant of perceived value is users' information security self-efficacy. It was obtained that people with

Table 5. Results.

Hypothesis	Path coefficient (Beta)	T-value	Support
H1a: The usefulness of users' perceived information security protection-> the value of perceived information security protection. (+)	0.38	4.86***	Y
H1b: Users' perceived information security threats-> the value of perceived information security protection. (+)	0.19	3.40***	Y
H2a: The perceived expense of users' information security protection mechanism-> the perceived value of their information security protection mechanism. (-)	(0.18)	2.96**	Y
H2b: The perceived impact of users' information security protection mechanism on system performance-> the perceived value of their information security protection mechanism. (-)	(0.18)	2.51*	Y
H2 c: The perceived barriers of users' information security protection mechanism-> the perceived value of their information security protection mechanism. (-)	0.01	0.11	N
H3:The perceived value of BYOD information security protection mechanism-> the intention to protect information security. (+)	0.44	9.09***	Y
H4:Users' BYOD information security awareness-> users' perceived value of information security protection mechanism. (+)	0.04	0.49	N
H5: Users' BYOD information security awareness-> users' intentions to protect information security. (+)	0.38	4.72***	Y
H6:Users' self-efficacy of BYOD information security-> users' perceived value of BYOD information security protection. (+)	0.15	1.97*	Y
H7:Users' self-efficacy of BYOD information security-> the intention to protect the information security. (+)	0.13	1.74	N

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$
Y: Supported; N: Non-supported

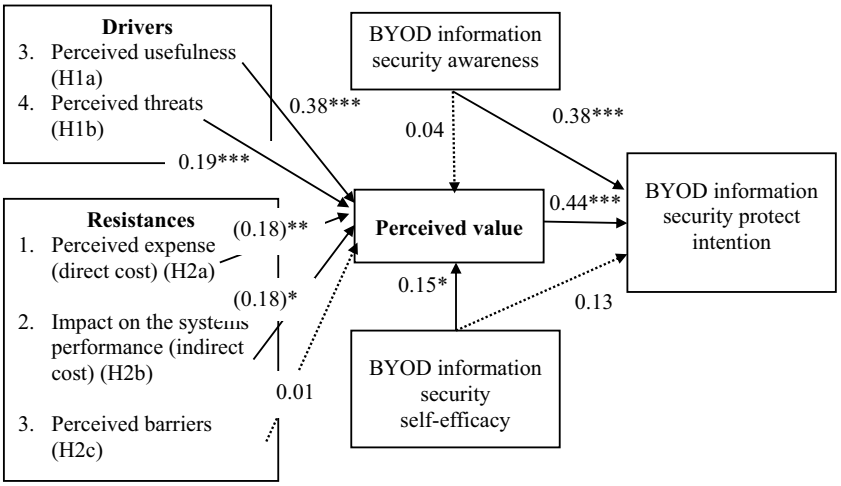

Figure 2. PLS structural results. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

higher self-efficacy demonstrate higher perceived value (Vekiri and Chronaki 2008). The results of this study also relate to the above opinion. Meanwhile, it differs from the results proposed in the work of Dang-Pham and Pittayachawan (2015) for the direct effect on intention. Consequently, businesses should provide information security-related education programs to promote the employees' information security self-efficacy. However, another interesting finding in this study is that BYOD information security awareness has no significant effect on perceived value (H4 is non-supported) but affects BYOD information security protecting intention significantly (H5 is supported). This means that both security awareness and self-efficacy are critical but the

effect varies. Self-efficacy refers to operational confidence and perceptions. Hence, users with higher self-efficacy towards information security protection have higher perceived value for the protection mechanism. On the contrary, awareness refers to the mindset perceptions, they feel its importance will do it. Thus, businesses should design educational programs to enhance employees' intentions. There is a need to identify the above differences. For the awareness level, we propose the provision of the conceptual programme to promote employee's mindset towards BYOD information security. In contrast, skill level education program enhances employees' self-efficacy towards the operation of the mechanisms. This is one of the contributions to the practice.

Based on the above findings, this study has the following contributes:

6.1 Theoretical contributions

Soomro, Shah, and Ahmed (2016) encourage the study of the managerial role of information security management. They investigated the human role when considering the information security management. Aguboshim and Udobi (2019) studied the importance of security issues towards mobile BYOD, relating to different traditional PC-based IS environment. In the present study, after reviewing the related theories towards information security management in the IS management field, TTAT (Liang and Xue 2009, 2010) represents the key theoretical background. However, they are two research differences obtained. Firstly, TTAT established under the PC era, but mobile IT or BYOD is a new paradigm shift. Further study is required to understand the model applicability. Liang and Xue (2009, 2010) discovered an issue between the voluntary technology avoidance behaviour and adoption in organisational settings. In other words, it means the spectrum between voluntary and mandatory. This study considers the SMEs which is within these points. SMEs have information security protection needed but different from large businesses with well-defined policies for compliance. It is a combination of voluntary and mandatory.

This study has academic value and application since it integrates two theories (TTAT and VAM) to understand new contexts: BYOD in SMEs. Besides the difference in the traditional PC environment, we focus on BYOD with cloud computing applications. The study identifies various paths of awareness and self-efficacy towards the intention of BYOD information security protection. Also, perceived value serving as the core construct in the proposed model is different from previous studies. The R^2 supports the theoretical contributions of this study.

6.2 Implications for practice

In the past few years, efforts in developing cloud services and promoting the use of mobile devices and services has been made in Taiwan. The report by the Institute for Information Industry, Taiwan (III) in 2015 showed that the penetration of smartphones was as high as 73.4% and that of tablets as high as 32%. Over 16 million people use these devices (Su, 2015). Taiwan's experience in managing BYOD information security serves as a reference for other countries, especially for Asian countries.

The results also contribute to the business community. Within corporates, BYOD has become a significant trend, which imposes new challenges on the management of

information security. Baillette, Barlette, and Leclercq-Vandelannoitte (2018) emphasised the different logic between traditional IT top-down adoption and BYOD bottom-up reversed adoption. In summary, corporates may enjoy a higher probability of success, reducing the risks, and costs of introducing BYOD into their systems. Besides, managerial knowledge and skills about information security management are important in managing a business (Haqaf and Koyuncu 2018). Therefore, the results of this study contribute to the understanding of users' perceptions towards BYOD information security protection, to enrich the knowledge, and skills about practical needs.

Finally, it was obtained that businesses manufacturing information security products helps in understanding of consumers' awareness and behaviour, thereby promoting their product development and marketing. Also, they understand how to increase users' perceived value of their product and promote to purchase.

6.3 Limitations and future research direction

Despite the significant findings of this study, it has some limitations. One of the limitations of this study is that its subjects were from an online forum. Although this has a certain degree of representation, however, it does not represent a sample from the broader population. This can be considered and improved in any future study. The data used in this study were only from Taiwan. However, different countries have various IT infrastructure and security threats. People from different countries also have differences in awareness and self-efficacy. The cost of security protection mechanisms also varies considerably. Therefore, cross-country comparisons will be needed in the future. Hence, this gives rise to the second limitation of this study.

7. Conclusions

The major working environment in smart and SMEs business is the BYOD with cloud-based applications. Different from traditional PC-based environment, new issues emerge from education and practice. Baillette, Barlette, and Leclercq-Vandelannoitte (2018) emphasised the different logic between traditional IT top-down adoption and BYOD bottom-up reversed adoption. Besides, they indicated the critical role of security problem organised when adopting BYOD. Soomro, Shah, and Ahmed (2016) studied the managerial role of information security management. They emphasised the human role when discussing the information security management. However, the above studies do not provide empirical results. Hence, the empirical study about BYOD information security protection is required. This study uses the empirical results to verify the integrated model. We indicated the determinants of the perceived value of BYOD information security protection. Also, we illustrated the difference affecting paths of awareness and self-efficacy relating to the behavioural intention to protect. The results also show the similarities and differences between previous studies. These results can serve as the references for the future academic study and practice.

Acknowledgments

The author would like to thank the Ministry of Science and Technology of Republic of China, Taiwan, for financially supporting this research under contract No. MOST 106-2410-H-025-009 – and MOST 108-2410-H-025-027 -

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the Ministry of Science and Technology of Republic of China, Taiwan [MOST 106-2410-H-025-009 – and MOST 108-2410-H-025-027].

References

Agrawal, N., and S. Tapaswi. 2019. "A Trustworthy Agent-based Encrypted Access Control Method for Mobile Cloud Computing Environment." *Pervasive and Mobile Computing* 52 (January): 13–28. doi:10.1016/j.pmcj.2018.11.003.

Aguboshim, F. C., and J. I. Udobi. 2019. "Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD)." *Journal of Information Engineering and Applications* 8 (1): 56–66.

Ahmed, E., I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, A. V. Vasilakos et al. 2017. "The Role of Big Data Analytics in Internet of Things." *Computer Networks* 129 (24): 459–471. DOI:10.1016/j.comnet.2017.06.013.

Allam, S., S. V. Flowerday, and E. Flowerday. 2014. "Smartphone Information Security Awareness: A Victim of Operational Pressures." *Computers & Security* 42 (May): 56–65. doi:10.1016/j.cose.2014.01.005.

Anderson, A., and A. Agarwal. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions." *MIS Quarterly* 34 (3): 613–643. doi:10.2307/25750694.

Baillette, P., Y. Barlette, and A. Leclercq-Vandelannoitte. 2018. "Bring Your Own Device in Organizations: Extending the Reversed IT Adoption Logic to Security Paradoxes for CEOs and End Users." *International Journal of Information Management* 43 (December): 76–84. doi:10.1016/j.ijinfomgt.2018.07.007.

Bandura, A. 1977. *Social Learning Theory*. Alexandria, VA: Prentice Hall.

Bauer, S., and E. W. N. Bernroider. 2017. "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization." *The DATA BASE for Advances in Information Systems* 48 (3): 44–68. doi:10.1145/3130515.3130519.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat 2009, August. "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy." Poster session presentation at the meeting of the 15th Americas Conference on Information Systems, pp. 419, San Francisco, CA. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1409&context=amcis2009.

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): 523–5489. doi:10.2307/25750690.

Cho, V., and W. H. Ip. 2018. "A Study of BYOD Adoption from the Lens of Threat and Coming Appraisal of Its Security Policy." *Enterprise Information Systems* 12 (6): 695. doi:https://doi.org/10.1080/17517575.2017.1404132.

Chu, C. W., and H. P. Lu. 2007. "Factors Influencing Online Music Purchase Intention in Taiwan: An Empirical Study Based on the Value-intention Framework." *Internet Research* 17 (2): 139–155. https://www.emerald.com/insight/content/doi/10.1108/10662240710737004/full/html.

Dang-Pham, D., and S. Pittayachawan. 2015. "Comparing Intention to Avoid Malware across Contexts in A BYOD-enabled Australian University: A Protection Motivation Theory Approach." *Computers & Security* 48 (February): 281–297. doi:10.1016/j.cose.2014.11.002.

Dillman, D. A. 1978. *Mail and Telephone Surveys: The Total Design Method*. New York: John Wiley & Sons.

Dillman, D. A. 2000. *Mail and Internet Surveys: The Tailored Design Method*. NJ, US: John Wiley & Sons.

Garba, A. B., J. Armarego, and D. Murray. 2015. "Bring Your Own Device Organizational Information Security and Privacy." *ARPN Journal of Engineering and Applied Sciences* 10 (3): 1279–1287.

Garba, A. B., J. Armarego, D. Murray, and W. Kenworthy. 2015. "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environment." *Journal of Information Privacy and Security* 11 (1): 38–54. doi:https://doi.org/10.1080/15536548.2015.1010985.

Gens, F. et al. 2019. IDC FutureScape: Worldwide IT Industry 2020 Predication. Framingham: International Data Corporation (IDC).

Granlien, M. S., and M. Hertzum. 2012. "Barriers to the Adoption and Use of an Electronic Medication Record." *Electronic Journal of Information Systems Evaluation* 15 (2): 216–227.

Hair, J. F., W. C. Black, B. J. Babin, and R. E. Anderson. 2014. *Multivariate Data Analysis*. London: PEARSON.

Haqaf, H., and M. Koyuncu. 2018. "Understanding Key Skills for Information Security Managers." *International Journal of Information Management* 43 (December): 165–172. doi:10.1016/j.ijinfomgt.2018.07.013.

Harris, M. A., K. Patten, and E. Regan 2013, August. "The Need for BYOD Mobile Device Security Awareness and Training." Poster session presentation at the meeting of the 19th Americas Conference on Information Systems, Chicago, IL.

Hayajneh, T. B. J. Mohd, A. Itradat, and A. N. Quttoum. 2013. "Performance and Information Security Evaluation with Firewalls." *International Journal of Security and Its Applications* 7 (6): 355–372. DOI:10.14257/ijsia.2013.7.6.36.

Hong, J. C., P. H. Lin, and P. C. Hsieh. 2017. "The Effect of Consumer Innovativeness on Perceived Value and Continuance Intention to Use Smartwatch." *Computers in Humane Behavior* 67 (February): 264–272. doi:10.1016/j.chb.2016.11.001.

Hsu, C. L., and J. C. C. Lin. 2015. "What Driver Purchase Intention for Paid Mobile Apps? – An Expectation Confirmation Model with Perceived Value." *Electronic Commerce Research and Applications* 14 (1): 46–57. doi:10.1016/j.elerap.2014.11.003.

Hsu, J. S. C. 2014. "Understanding the Role of Satisfaction in the Formation of Perceived Switching Value." *Decision Support Systems*. 59: 152–162. March. https://www.sciencedirect.com/science/article/pii/S0167923613002637

Huang, D. L., P.-L. Patrick Rau, G. Salvendy, F. Gao, and J. Zhou. 2011. "Factors Affecting Perception of Information Security and Their Impacts on IT Adoption and Security Practices." *International Journal of Human-computer Studies* 69 (12): 870–883. doi:10.1016/j.ijhcs.2011.07.007.

Ibrahim, A., Y. C. Yasemin, and T. Ozgur. 2015. "Impact of Perceived Security on Organizational Adoption of Smartphones." *Cyberpsychology, Behavior and Social Networking* 18 (10): 602–608. doi:https://doi.org/10.1089/cyber.2015.0243.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95. doi:10.1016/j.cose.2011.10.007.

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.

Kadimo, K., M. B. Kebaetse, D. Ketshogileng, L. E. Seru, K. B. Sebina, C. Kovarik, and K. Balotlegi. 2018. "Bring-your-own-device in Medical Schoo.ls And Healthcare Facilities: A Review of the Literature." *International Journal of Medical Informatics* 119: 94–102. doi:https://doi.org/10.1016/j.ijmedinf.2018.09.013.

Khan, A. N., M. L. Mat Kiah, S. U. Khan, and S. A. Madani. 2013. "Towards Secure Mobile Cloud Computing: A Survey." *Future Generation Computer Systems* 29 (5): 1278–1299. doi:10.1016/j.future.2012.08.003.

Kim, H. W., H. C. Chan, and S. Gupta. 2007. "Value-based Adoption of Mobile Internet: An Empirical Investigation." *Decision Support Systems* 43 (1): 111–126. doi:https://doi.org/10.1016/j.dss.2005.05.009.

Kim, Y. H., D. Kim, and K. Wachter. 2013. "A Study of Mobile User Engagement (Moen): Engagement Motivations, Perceived Value, Satisfaction, and Continued Engagement Intention." *Decision Support Systems* 56 (December): 361–370. doi:10.1016/j.dss.2013.07.002.

Kruger, H. A., and W. D. Kearney. 2006. "A Prototype for Assessing Information Security Awareness." *Computers & Security* 25 (4): 289–296. doi:10.1016/j.cose.2006.02.008.

Kshetri, N. 2013. "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution." *Telecommunications Policy* 37 (4–5): 372–386. doi:10.1016/j.telpol.2012.04.011.

Lebek, B., J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler 2013, January. "Employees' Information Security Awareness and Behavior: A Literature Review." Poster session presentation at the meeting of the 46th Hawaii International Conference on System Sciences, pp. 2978–2987, Hawaii, USA.

Lebek, B., K. Degirmenci, and M. H. Breitner 2013, August. "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices." Poster session presentation at the meeting of the 19th Americas Conference on Information Systems, Chicago, IL.

Lee, J., M. Warkentin, R. E. Crossler, and R. F. Otondo. 2017. "Implications of Monitoring Mechanisms on Bring Your Own Device Adoption." *Journal of Computer Information Systems* 57 (4): 309–318. doi:10.1080/08874417.2016.1184032.

Li, L., W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan. 2019. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior." *International Journal of Information Management* 45 (April): 13–24. doi:10.1016/j.ijinfomgt.2018.10.017.

Liang, H., and Y. Xue. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective." *MIS Quarterly* 33 (1): 71–90. doi:10.2307/20650279.

Liang, H., and Y. Xue. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *Journal of the Association for Information Systems* 11 (7): 394–413. doi:10.17705/1jais.00232.

Lin, T. C., S. Wu, J. S. C. Hsu, and Y. C. Chou. 2012. "The Integration of Value-based Adoption and Expectation–confirmation Models: An Example of IPTV Continuance Intention." *Decision Support Systems* 54 (1): 63–75. doi:https://doi.org/10.1016/j.dss.2012.04.004.

Liu, F., X. Zhao, P. Y. K. Chau, and Q. Tang. 2015. "Roles of Perceived Value and Individual Differences in the Acceptance of Mobile Coupon Applications." *Internet Research* 25 (3): 471–495. https://www.emerald.com/insight/content/doi/10.1108/IntR-02-2014-0053/full/html.

Morrow, B. 2012. "BYOD Security Challenges: Control and Protect Your Most Sensitive Data." *Network Security* 2012 (12): 5–8. doi:10.1016/S1353-4858(12)70111-3.

Mylonas, A., A. Kastania, and D. Gritzalis. 2013. "Delegate the Smartphone User? Security Awareness in Smartphone Platforms." *Computers & Security* 34 (May): 47–66. doi:10.1016/j.cose.2012.11.004.

Ng, B. Y., A. Kankanhalli, and Y. Xu. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective." *Decision Support Systems* 46 (4): 815–825. doi:https://doi.org/10.1016/j.dss.2008.11.010.

Olalere, M., M. T. Abdullah, R. Mahmod, and A. Abdullah. 2015. "A Review of Bring Your Own Device on Security Issues." *SAGE Open* 5 (2): 1–11. doi:10.1177/2158244015580372.

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram. 2014. "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)." *Computers & Security* 42 (May): 165–176. doi:10.1016/j.cose.2013.12.003.

Putri, F., and A. Hovav 2014, June. "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory." Poster session presentation at the meeting of the Twenty Second European Conference on Information Systems, Tel Aviv, Israel.

Ramachandran, M. 2016. "Software Security Requirements Management as an Emerging Cloud Computing Service." *International Journal of Information Management* 36 (4): 580–590. doi:10.1016/j.ijinfomgt.2016.03.008.

Ramachandran, M., and V. Chang. 2016. "Toward Performance Evaluation of Cloud Service Providers for Cloud Data Security." *International Journal of Information Management* 36 (4): 618–625. doi:10.1016/j.ijinfomgt.2016.03.005.

Rezgui, Y., and A. Marks. 2008. "Information Security Awareness in Higher Education: An Exploratory Study." *Computers & Security* 27 (7–8): 241–253. doi:10.1016/j.cose.2008.07.008.

Rhee, H. S., C. Kim, and Y. U. Ryu. 2009. "Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior." *Computers & Security* 29 (8): 816–826. doi:https://doi.org/10.1016/j.cose.2009.05.008.

Ringle, C. M., M. Sarstedt, and D. W. Straub. 2012. "Editor's Comments: A Critical Look at the Use of PLS-SEM in MIQ Quarterly." *MIS Quarterly* 36 (1): iii–xiv. doi:10.2307/41410402.

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

Samonas, S., G. Dhillon, and A. Almusharraf. 2020. "Stakeholder Perceptions of Information Security Policy: Analyzing Personal Constructs." *International Journal of Information Management* 50 (February): 144–154. doi:10.1016/j.ijinfomgt.2019.04.011.

Sari, P. L., and Candiwan. 2014. "Measuring Information Security Awareness of Indonesian Smartphone Users." *TELKOMNIKA* 12 (2): 493–500. doi:10.12928/telkomnika.v12i2.64.

Siponen, M. T. 2000. "A Conceptual Foundation for Organizational Information Security Awareness." *Information Management & Computer Security* 8 (1): 31–41. doi:10.1108/09685220010371394.

Soomro, Z. A., M. H. Shah, and J. Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36 (2): 215–225. doi:10.1016/j.ijinfomgt.2015.11.009.

Steelman, Z. R., M. Lacity, and R. Sabherwal. 2016. "Charting Your Organization's Bring-your-own-device Voyage." *MIS Quarterly Executive* 15 (2): 85–104.

Su, W. B. 2015. Over 16 Million People Use Smart Mobile Devices in Taiwan. Accessed 8 July 2020. https://www.ithome.com.tw/news/97479

Tarekegn, G. B., and Y. Y. Munaye. 2016. "Big Data: Security Issues, Challenges and Future Scope." *International Journal of Computer Engineering & Technology* 7 (4): 12–24.

Thenral, E., and L. Suganthi. 2018. "Product Involvement and Self-efficacy on Perceived Value of Co-design." *Anthropologist* 34 (1–3): 20–27.

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory." *Information & Management* 49 (3–4): 190–198. doi:10.1016/j.im.2012.04.002.

Vekiri, I., and A. Chronaki. 2008. "Gender Issues in Technology Use: Perceived Social Support, Computer Self-efficacy and Value Beliefs, and Computer Use beyond School." *Computers & Education* 51 (3): 1392–1404. doi:10.1016/j.compedu.2008.01.003.

Wang, Y. S., C. H. Yeh, and Y. W. Liao. 2013. "What Drives Purchase Intention in the Context of Online Content Services? the Moderating Role of Ethical Self-efficacy for Online Piracy." *International Journal of Information Management* 33 (1): 199–208. doi:https://doi.org/10.1016/j.ijinfomgt.2012.09.004.

Weeger, A., X. Wang, and H. Gewald. 2016. "IT Consumerization: BYOD-program Acceptance and Its Impact on Employer Attractiveness." *Journal of Computer Information Systems, Vol* 56 (1): 1–10. doi:10.1080/08874417.2015.11645795.

Weeger, A., X. Wang, H. Gewald, M. Raisinghani, O. Sanchez, G. Grant, and S. Pittayachawan. 2018. "Determinants of Intention to Participate in Corporate BYOD-programs: The Case of Digital Natives." *Information Systems Frontiers*. doi:https://doi.org/10.1007/s10796-018-9857-4.

Wipawayangkool, K. 2009. "Exploring the Nature of Security Awareness: A Philosophical Perspective." *Issues in Information Systems* X (2): 407–414.

Workman, M., W. H. Bommer, and D. Straub. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test." *Computers in Human Behavior* 24 (6): 2799–2816. doi:10.1016/j.chb.2008.04.005.

Yang, H., J. Yu, H. Zo, and M. Choi. 2016. "User Acceptance of Wearable Devices: An Extended Perspective of Perceived Value." *Telematics and Informatics* 33 (2): 256–269. doi:10.1016/j.tele.2015.08.007.

Yu, J., H. Lee, I. Ha, and H. Zo. 2017. "User Acceptance of Media Tablets: An Empirical Examination of Perceived Value." *Telematics and Informatics* 34 (4): 206–223. doi:10.1016/j.tele.2015.11.004.

Zulhuda, S., I. M. A. G. Azmi, and N. Hakiem. 2015. "Big Data, Cloud and Bring Your Own Device: How the Data Protection Law Addresses the Impact of "Datafication"." *Advanced Science Letters* 21 (10): 3347–3351. doi:10.1166/asl.2015.6493.

ZyXEL, T. K. 2015. "The SME Security Challenge." *Computer Fraud & Security* 2015 (3): 5–7.