February, 2015

Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach

Duy Dang-Pham, *RMIT University*
Siddhi Pittayachawan, *RMIT University*

Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach

Duy Dang-Pham and Siddhi Pittayachawan
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: duy.dang@rmit.edu.au; siddhi.pittayachawan@rmit.edu.au

ABSTRACT

Malware have been regarded as a persistent threat to both individuals and organisations due to its wide spread via various means of infection. With the increasing use of personal mobile devices and the trending adoption of Bring Your Own Device (BYOD) practices, this threat has become even more versatile and dreadful as it could hide behind the users' typical and daily Internet activities. The importance of investigating whether the user's intention to perform malware avoidance behaviours would change across multiple contexts is emphasised. Consequently, this study determines the contributing factors and compares their impacts on such intention by extending Protection Motivation Theory in two different contexts. A total of 252 Australian higher education students were surveyed when using mobile devices such as smartphone, laptop and tablet at home and at a BYOD-enabled university. Paired *t*-test, Bayesian structural equation modeling, and revised *z*-test were employed for data analysis. The empirical findings reveal that intention to perform malware avoidance behaviours differed across the contexts. Furthermore, the researchers found perceptions of self-efficacy and vulnerability to have different impacts on such intention and other variables in the model. As a result, such findings suggested developing community of practice and repeated trainings to maintain the users' confidence in their own abilities to cope with malware threats. Message that focuses on the threats' consequences was suggested to improve home users' intention to avoid malware, along with a number of factors that could be critical to designing information security education programs. Moreover, these implications particularly address information security management at educational institutions that adopt BYOD policy. Finally, theoretical contributions include an extended model based on Protection Motivation Theory that reflects the users' intention to avoid malware threats in BYOD context, from which directions for future research were also provided.

Keywords: malware, information security behaviour, protection motivation theory, BYOD, Bayesian structural equation modeling

1. INTRODUCTION

Organisations and individuals have been constantly facing online threats as they rely more on the emerging technologies. More recently, much attention is being raised to a range of malware threats such as cyberespionage, cyber-sabotage and stealing confidential information (Symantec, 2013). Malware is software that has the abilities to take control and damage computers (Google, 2013) and they were used in the data breaches that have costed billions of dollars globally in 2011 (Ponemon Institute, 2012; Symantec, 2013). In particular of this study's context, Australian organisations alone suffered heavy data breaches that costed USD 2,270,862 on average (Ponemon Institute, 2012), and the spreading of malware infections is persistent and growing more sophisticated in methods along with the technological trends.

There has always been a continuous demand for research on information security behaviours (Crossler et al. 2013; Willison and Warkentin 2013). Despite more studies (e.g. Herath and Rao, 2009; Johnston and Warkentin, 2010; Lee et al., 2008; Vance et al., 2012) have investigated the users' intention to perform information security behaviours in the last few years, there are issues in the field that require urgent attention. These include the shortage of research investigating information security behaviours in multiple contexts, rather than one at a time, especially in home environment (Li and Siponen, 2011). In fact, the growing use of personal mobile devices and adoption of Bring Your Own Device (BYOD) policy suggest that even security mistakes at non-work contexts may affect the organisation's or public places' online safety. In other words, both individuals and their associated organisations would be constantly facing cyber-threats.

Those information security issues have been particularly emphasised in the recent body of knowledge, as the Editor-in-Chief of Computers & Security journal has mentioned in the 2013 editorial letter: "… disruptions of good security at organisations because of BYOD (Bring Your Own Device) not being appropriately controlled." (Spafford, 2013, p. v) More important, specific problems concerning the use of emails and social media platforms such as malware, spam and phishing, difficulty of achieving user's compliance and social engineering still persist over time (Spafford, 2013). Similarly, the case studies in Silic and Back's (2014) research revealed that organisations are facing enormous difficulties in controlling the increased security risks of "mobile shadow IT" behaviours, resulting from BYOD adoption such as the users installed unauthorised software on their own devices while believing they are not doing anything wrong. Nonetheless, managing the end-users' varied levels of information security awareness and mitigation skills when using mobile devices in BYOD-enabled organisations is a daunting task (Allam et al., 2014). In fact, Silic and Back (2014) discussed that restriction in BYOD-enabled environments is a valid countermeasure but not a solution for such risks, and this present article agrees with this perspective. As a consequence, it is contended that the key to good security of BYOD-enabled environments must rely heavily on the voluntary threats avoidance or protection of personal mobile devices' users. Subsequently, such behaviours depend on how well the users perceive the threats as well as the coping solutions to those threats, which are currently an unanswered question and therefore raise the need for an investigation. As a result, it motivates the researchers to conduct this study which aims at understanding such perceptions of the users in a BYOD-enabled environment.

To achieve the research objective, the researchers surveyed 252 higher education (HE) students from a BYOD-enabled university in Australia and developed a conceptual model to explain how intention to perform malware avoidance behaviours changed across contexts i.e. at home and at BYOD-enabled environment. Since HE students are within the ages range of the user group exposing most to malware threats and they would become the next workforce soon, surveying for their insights would be relevant and justified. Furthermore, this study forwards an appropriate research method to test and compare intention to perform information security behaviours across multiple contexts, which has not been done by prior studies and recently demanded future research's attention (Li and Siponen, 2011). In details, Paired *t*-test and multiple-group Bayesian structural equation modeling are employed to detect and measure the different contributing impacts towards intention to perform across the contexts. The researchers believe this study could be considered as important and significant, given its relevant contributions to the emerging topics in the current body of information security knowledge. Ultimately, the study seeks to answer the research questions:

1. Does the user's intention to perform malware avoidance behaviours change across contexts when using personal mobile devices?
2. What are the contributing factors and their impacts on the user's intention to perform malware avoidance behaviours when using personal mobile devices?

2.1. To what extent the impacts on such intention have changed across contexts?

2. LITERATURE REVIEW

2.1. The emerging malware threats of non-work activities in BYOD environment

At the moment, malware threats are becoming more diversified and specialised–far away from the traditional infection from malicious emails' links and attachments–especially in the domains of online social networks (OSN) and mobile devices (Sophos, 2014). For instance, there are social media methods that exploit the functions of OSNs to disseminate malware through typical activities such as offering fake gift cards or tricking OSN users to share the appealing, malware-embedded videos, websites or messages (Symantec, 2013). In addition, Symantec (2013) found a swelling number of mobile malware families that increased 58% since 2011, resulted in 415 vulnerabilities in 2012. It would be reasonable to argue that today's rapid adoption of mobile devices make the users exposed more to both traditional and emerging malware threats from emails and OSNs since they could perform those typical activities on their devices everywhere at any time.

On the other hand, it is evident that the malware threats are extending their reach to non-work activities. It is also worth mentioning that the term *non-work* activities used throughout this study is consistent with Li and Siponen's definition (2011 pp. 5–6), which refers to activities performed for personal purpose (e.g. online shopping, playing online games, web chatting, downloading software and music, and so on). More specifically in this research's context, Australian users reported a high amount of non-work Internet use on checking emails (95%), browsing websites (88%) and downloading files (63%) either on desktop computers or mobile devices (AusCERT, 2008). Furthermore, the young-adult Australian population appears to increasingly dominate in using the Internet for those activities. For instance, their online activities include "browsing websites or search for information" (90%), "used a social networking site" (71%), "downloaded audio or video content" (33%) and "purchased goods or services" (33%) (ACMA, 2013). As a consequence, it is clear that Australian young-adults are highly exposed to the malware threats behind these non-work Internet activities.

The spread of malware infection could be argued to be extended even further by the increasing adoption of Bring Your Own Device (BYOD) policy. BYOD is a management policy that allows the users to access work resources and applications from their personal mobile devices (e.g. laptops, smartphones and tablets). In particular to the higher education sector, BYOD could reduce the purchasing and maintenance costs of IT infrastructure by enforcing students to bring personal mobile devices for their studies (Hamza and Noordin, 2013). They also found adoption of BYOD policy improved postgraduates' academic efficiency in terms of professional competency, accelerating research progress and stimulating learning. As a result, countries such as Australia where there is a high Internet penetration rate of 88.8% started adopting and enforcing BYOD practices (Internet World Stats, 2014). For instance, the Department of Education in New South Wales requires schools to support BYOD policy (NSW Government, 2014). Similarly, other states such as Queensland and Victoria also advocates BYOD adoption (Northern Grampians Council, 2013; Office of the Information Commissioner Queensland, 2014). Furthermore, the trending adoption of BYOD policies has come to the attention of Australian government that a report outlining the considerations regarding BYOD was published recently (Australian Government, 2014).

Nevertheless, the downsides of BYOD policy include a number of information security risks such as insecure use of a large volume of endpoints (Gajar et al., 2013; Miller et al., 2012) or loss or theft of the employees' personal devices (Burt, 2011; Jain and Shanbhag, 2012). The recent report about Australian's password use and management (Centre for Internet Safety, 2011) reveals that 36% of Australian chose to remain logged-in their online accounts on mobile phones while 60% of them used the same password across one or more online accounts. Given such state, it would not be much challenging for the cyber-criminals to acquire the passwords to multiple accounts if the mobile device was stolen or hijacked.

Last but not least, the recent insights from information security experts indicated that the new generations of today's workforce are strongly advocating the use of personal mobile devices at workplaces and expecting BYOD policy to be adopted by their future employers (Mansfield-Devine, 2012; Thomson, 2012). In this case, it would be likely to expect that most Australian organisations (or any countries with high volume of mobile devices' use by the youths) have to face the BYOD's malware threats in the near future. In addition, the personal mobile devices could be infected by malware at any places to where the corporate's professional network security cannot extend its protection. As a result, it appears that the overall online safety of both individuals and organisations relies more on the information security behaviours of the mobile devices' owners, rather than the protection technologies.

2.2. Potential differences in intentions to avoid malware at university and at home

As argued previously, today's information security against malware is becoming more dependent on adequate security behaviours performed by the users in both well-protected public places and less secured home environment. Nevertheless, the current literature has yet to fully measure how well information security behaviours are invariant or change across contexts. In fact, few studies were found to share such concern but Li and Siponen's research (2011) which theorises the potential differences in information security behaviours into four contexts: (1) *work at workplace,* (2), *work at home*, (3) *non-work at home* and (4) *non-work at workplace*. Since this research's focus is about malware threats in *non-work* Internet activities, it will concentrate on contexts (3) and (4). Before discussing in-depth the differences between these two contexts and how they would affect information security behaviours, the researchers replaced "workplace" context with "university".

A number of recent literature has discussed BYOD practices in universities around the world (e.g. Adhikari et al., 2006; Barkhuus, 2005; Hamza and Noordin, 2013; Nykvist, 2012), which makes BYOD a trending policy in the educational sector. In fact, the university where this research took place has also been adopting BYOD policy recently. While BYOD adoption varies across industries and sectors, the researchers argue that the adoption of this policy in universities and common workplaces may share similar characteristics regarding information security. To start with, Markelj and Bernik (2012) and Romer (2014) summarised the best practices of securing mobile use by modern BYOD-enabled companies which include mobile devices management (MDM) systems, enforcing safety regulations, centralising access control and monitoring as well as blocking risky services. While there is a lack of literature describing information security for BYOD-enabled educational institutions, studies from the education field have proposed solutions common to those used in other industries.

For instance, Vesey (2013) reported that blocked access to Web 2.0 websites such as Facebook and YouTube were implemented by the university. On the other hand, Samochadin et al. (2014) and Emery (2012) proposed the use of MDM systems and techniques (e.g. educate users, design policy, require registration of mobile devices and allow remote access if necessary) to improve information security for personal mobile devices of staff and students in the BYOD-enabled campus. Likewise, Lennon (2012) detailed the security infrastructure being implemented in their campus which includes having IT department to install security controls on the users' mobile devices, security policies and awareness training. However, the author was concerned with risky behaviours such as loaning devices to the others, failing to use anti-virus software to check and encrypt files, as well as the users' perceived difficulty to locate security policies in the campus (Lennon, 2012). More concerns about security issues in the campus were found mainly in the fear of lost or stolen mobile devices from both the students and the security staff's perspectives, besides the emerging cyber-threats (Bidin and Ziden, 2013; Kobus et al., 2013). Bidin and Ziden (2013) further noted that currently there is a lack of standard solutions to cope with stalking, identity theft and cyber-bullying at BYOD-enabled universities. The users are then suggested to mitigate the risks by their own through receiving the tips and advice to do so (Bidin and Ziden, 2013).

In summary, the discussed studies displayed the common concerns and viewpoints about information security solutions for BYOD-enabled environments shared by the educational sector and other industries. As a result, the researchers believe that this study's analyses on the data collected from the HE students would remain intact, and the comparison of the two contexts would not deviate much from the originals as long as the focal activities remain the same as *non-work*. In exchange, comparing university against home contexts allowed this study to precisely measure the perceptions of the students about performing malware avoidance behaviours in their own real environments. The differences in performing secured *non-work* Internet activities between university and home contexts are elaborated below.

2.2.1. *Performing non-work Internet activities at university*

According to Li and Siponen (2011), *policy*, *sanction* and *monitoring* are the contextual factors that would help the users to perform proper information security behaviours in corporate environment. Specifically, organisational policy could instruct safe practices to the users, along with sanction and monitoring that raise awareness about the consequences of performing abusive behaviours (Li and Siponen, 2011). Likewise, the university in this study also provides guidance and policies that support the students' use of personal mobile devices. On the other hand, it is recognised that sanction and monitoring could exhibit weaker effects in university than in workplace's environment. This is because the students are not bound to formal contract and serious punishments as compared to workplaces. In fact, the university policy states that IT violations can only result in disciplinary action and dismissal but only referral to appropriate authorities if it is considered as an extreme case. Nevertheless, the unique existences of these three contextual factors at university could differentiate the students' intention to perform malware avoidance behaviours as compared to home's context.

2.2.2. Performing non-work Internet activities at home

In contrast with university's context, the students should not be affected by policy, sanction and monitoring at home. However, the contextual factors *possible sharing computers* and *network security* could influence their intention to perform malware avoidance behaviours (Li and Siponen, 2011). For instance, maintaining online safety for a laptop at home would be challenging if family members having different knowledge about information security use it for various purposes. In addition, home's network security should not be able to achieve the same level of protection as compared with corporate's due to the lack of investment and infrastructure. Therefore, it is argued that the students would have to rely more on their vigilance and efforts at home to keep their personal mobile devices safe from malware.

From the above discussion, it is anticipated that the students' intention to perform malware avoidance behaviours would be different at home and at university due to the influences of those contextual factors. The next section reviews the relevant existing studies on information security behaviours performed at home and at public/workplace. The researchers also selected a suitable theory on which the conceptual model could be grounded. The model should be able to describe in details how intention to perform malware avoidance behaviours is formed, so that the potential changes during that process could be measured across the contexts.

2.3. Summary of extant research on information security behaviours

The previous section has introduced the emerging malware threats on personal mobile devices and discussed how it would threaten the BYOD-enabled environments, particularly if the users fail to maintain good malware avoidance behaviours across the different contexts of using mobile devices. This section summarises the current knowledge body of research which focuses on the contributing factors of desirable information security behaviours. More specifically, there is a growing interest in applying multidisciplinary theories to explain the relationships between such motivational factors and the users' behavioural intention. Among those studies, two distinctive groups focusing on home users and corporate employees' behaviours could be identified.

On one hand, Li and Siponen (2011) emphasised that there is currently a deficiency in research about home user's information security behaviours, despite their important role in the security chain. To start with, Ng and Rahim (2005) and Lee and Kozar (2008) investigated the impacts of Theory of Planned Behaviour's factors on home user's intention to perform protective behaviours such as using anti-virus/anti-spyware software, setting firewall and performing data backup. Both studies found significant motivational impacts of attitude, subjective norms and behavioural control on the users' behavioural intention. More interesting, Anderson and Agarwal (2010) explicitly studied the different effects of those factors on home user's security behaviours on the Internet and their own computer. As a consequence, attitude demonstrated significantly stronger impact towards intention to perform information security behaviours on home computer than on the Internet. Surprisingly, subjective norm only had small influence on home computer-oriented behaviours but not the Internet-oriented one (Anderson and Agarwal, 2010). Last but not least, Liang and Xue (2010) proposed the Technology Threat Avoidance Theory and tested it for home user's intention to adopt anti-spyware software. While the theory demonstrated strong prediction towards such intention, it is contended that there is still a need to understand what motivate the proactive behaviours such as carefully examining email contents or avoid clicking suspicious websites, rather than installing and relying on automatic software. Provided the scarce findings about home user's security behaviours discussed previously, little has been found regarding the motivations of the user's proactive behaviours while using the Internet.

On the other hand, a larger amount of studies were focusing on determining the motivations of corporate employee's intention to perform information security behaviours. Among the theories applied in this research group, Protection Motivation Theory (PMT) (Rogers, 1975) was found to play a dominant role in explaining the contributing factors of intention to perform desirable information security behaviours. For example, Herath and Rao (2009) and Vance et al. (2012) both tested the effects of PMT's factors on intention to comply with security policy. In Vance et al.'s study (2012), the theory demonstrated good explanatory power by explaining 44% of the behavioural intention, with five out of six PMT factors displayed statistically significant impacts. On the other hand, Herath and Rao (2009) tested partially the effects of PMT's factors while combining with other theories such as General Deterrence Theory and Theory of Planned Behaviour. The PMT's factors explained quite well the construct "attitude" which in turn explained 47% of the behavioural intention's total variance (Herath and Rao, 2009). The common adoption of PMT in information security research also reflected in examining the intention to adopt anti-virus software (Johnston and Warkentin, 2010; Lee et al., 2008). In Lee et al.'s (2008) study, PMT's factors were capable to explain 45% of the intention to install anti-virus software, while Johnston and Warkentin's model (2010) was accounted for 27% of the intention. In overall, PMT demonstrated stable and decent explanatory power towards intention to perform desirable information security behaviours, provided its original model had been tested as a whole or partially by integrating with other theories. Nevertheless, there is lacking evidences of PMT being applied in non-work context and for testing proactive behaviours.

The researchers choose to develop the conceptual model based on PMT and test it for malware avoidance behaviours performed by the students while using personal mobile devices for non-work purposes in two contexts. As discussed throughout the literature review section, ensuring information security in the BYOD-enabled environments would not just require the users' adherence to policies and installation of controls but also depend heavily on their own proactive security behaviours. For instance, the user's behaviour to proactively examine the email's content or avoid clicking suspicious websites is arguably much valuable whether there exists anti-virus software or not, and so is understanding the motivations of such behaviours. It is anticipated that the PMT model would produce reliable and comparable findings about the motivations.

3. HYPOTHESES DEVELOPMENT

Provided the research questions, the researchers developed two sets of hypotheses that aim to test (1) the contributing factors' effects on intention to perform malware avoidance behaviours when using personal mobile devices (e.g. laptop, tablet, and smartphone), and (2) the variance of the same effects in two different contexts. As a result, hypotheses in the first set will be assigned the initial H plus order number (e.g. H5 refers to hypothesis #5 about perceived vulnerability's contributing effect on intention), whereas hypotheses in the second set about the variances of the matching effects will be written in the same way plus the small letter "a" to differentiate them from the first set (e.g. H5a refers to the hypothesis that tests whether the contributing effect of perceived vulnerability on intention differs across two contexts). In summary, hypotheses without letter "a" test for significant effects of contributing factors on intention, while hypotheses with letter "a" test for significant variances of those effects.

This section begins with identifying the specific malware avoidance behaviours that the model will test for its intention's contributing factors. The four malware avoidance behaviours were selected based on their effectiveness and how they would be widely known by laypersons as recommended by Google's Good-to-know website about staying safe on the Internet (Google, 2013). These behaviours include *carefully examine sender's address and content while checking emails*, *avoid clicking on suspicious websites* and *lock the devices when stop using them*. Given the previous section that discusses how the users' intention would differ across contexts, it is hypothesised that:

- H1a: Intention to *carefully examine email sender's address* when using personal mobile devices differs across the contexts.
- H2a: Intention to *carefully examine email's content* when using personal mobile devices differs across the contexts.
- H3a: Intention to *avoid clicking malicious websites* when using personal mobile devices differs across the contexts.

- H4a: Intention to *lock devices when stop using them* when using personal mobile devices differs across the contexts.

Next, PMT elaborates through its model how the factors within the cognitive process of a person motivate his or her intention to perform certain behaviour. Specifically, two components of the cognitive process were mentioned in the original work of Rogers (1975), namely *threat appraisal* and *coping appraisal.* Each of these components has three cognitive factors which in turn help to explain how a person assesses both the threats and the solutions before forming the intention to perform such solutions to counter the threats.

Threat appraisal cognitive process: According to Rogers (1975) and its revised version (as described in Boer and Seydel 1996), the appraisal of a threat involves three cognitive factors which are *vulnerability*, *severity*, and *advantages of maladaptive behaviours*. Recent research, however, has been measuring a similar construct to the third factor, namely *rewards* (e.g. Mohamed and Ahmad, 2012; Siponen et al., 2007; Vance et al., 2012). As a result, *advantages of maladaptive behaviours* construct are hereby referred to as *rewards*.

The original PMT posited that when a person feel vulnerable against a threat, they would be more inclined to perform the recommended behaviours to counter such threat (Rogers, 1975). Similarly, it is argued that the users would intend more to perform malware avoidance behaviours if they perceive themselves to be vulnerable against the malware threats. On the other hand, the same motivating impact on *intention to perform* was found in *severity* (Rogers, 1975). As a result, the researchers hypothesised that the users' perception of malware's severity could motivate their intention to perform malware avoidance behaviours. Lastly, the factor *rewards* in this study represents the realised benefits of performing the malware-risky behaviours such as saving more time and efforts. Therefore, it is hypothesised that those *rewards* would reduce the intention to perform the adaptive behaviours. In summary, the researchers propose the following hypotheses.

- H5: Vulnerability (VUL) increases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.
- H6: Severity (SEV) increases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.
- H7: Rewards (REW) decreases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.

Coping appraisal cognitive process: parallel with the appraisal of threat is the evaluation of the coping behaviours which subsequently forms the intention to perform such behaviours (Rogers, 1975). Similar to threat appraisal process, the latest revised PMT describes three cognitive factors associating with the coping appraisal, namely *response efficacy*, *response cost* and *self-efficacy* (Boer et al., 1996).

Response efficacy and *response cost* constructs reflect the perceived characteristics of the coping behaviours. Specifically, it was posited in PMT that a person intends to perform the adaptive behaviours more as they perceive the behaviours to be effective (Rogers, 1975). In contrast, the costs of performing the behaviours (such as time loss or increased inconveniences) would in turn discourage the intention to perform (Rogers, 1975). On the other hand, the factor *self-efficacy* refers to the personal belief of one's ability to accomplish a task (Luszczynska and Schwarzer, 2005). PMT posited that a person with high *self-efficacy* would intend to perform the adaptive behaviours more (Rogers, 1975). As a result, the researchers hypothesised as below.

- H8. Response efficacy (REF) increases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.
- H9. Response cost (COS) decreases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.
- H10. Self-efficacy (SEF) increases intention to perform malware avoidance behaviours (ITA) when using personal mobile devices.

Finally, as the study's focal goal is to measure the extent of how much the cognitive process' impacts on intention to perform would change across contexts, additional hypotheses about the differences in the six hypothesised causalities were added.

- H5a: The impact of vulnerability (VUL) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.
- H6a: The impact of severity (SEV) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.

- H7a: The impact of rewards (REW) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.
- H8a: The impact of response efficacy (REF) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.
- H9a: The impact of response cost (COS) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.
- H10a: The impact of self-efficacy (SEF) on intention to perform malware avoidance behaviours (ITA) differs across the contexts.

4. RESEARCH DESIGN

4.1. Questionnaire design

The researchers developed the questionnaire from a three-step process. First, the four questions measuring the construct *Intention to perform malware avoidance behaviours* (ITA) were developed based on the behaviours from Google's Good-to-know website (Google, 2013) (displayed in Table A). The researchers selected the behaviours that would be familiar and easily performed to avoid malware threats by general Internet users (i.e. carefully examine email's content and sender's address; avoid clicking on malicious websites and lock devices). Second, the rest of the questions measuring PMT's constructs were designed by reviewing the facets of similar constructs from prior studies (Herath and Rao, 2009; Lee et al., 2008; Mohamed and Ahmad, 2012; Willison and Warkentin, 2013) (displayed in column "Question" in Table A). Third, pilot tests were conducted by two academics in the field and ten students to ensure content validity. In addition, discussions were made among the researchers and added into the pilot-tests' insights so to pick the most relevant and understandable measures (out of four facets per construct) for measuring the PMT constructs (displayed in column "Refined question" in Table 1). The researchers then asked these refined questions for the four malware avoidance behaviours, so that a construct would be measured by four items to avoid under-identification error and biased covariance in measurement model analysis as recommended by Kline (2011 pp. 358–359).

This process resulted in 28 questions measuring seven constructs of PMT. To collect data simultaneously per construct in both contexts, two scales per set of four questions were assigned–thereby creating a total of 56 questions. Six-point Likert scale was employed to collect data for MSEM while preventing them from giving "neutral" answers. Given such large amount of questions, the questionnaire was broken down into four sections: (1) demographics, (2) intention to perform malware avoidance behaviours, (3) threat appraisal, and (4) coping appraisal so to reduce the overwhelming perception of the respondents. The average pilot-tested time to complete the questionnaire was varied under 10 minutes and should not cause frustration to the respondents.

4.2. Data collection

Determining the appropriate sample size for structural equation modeling is challenging since it needs to balance between achieving statistical significance to reject the causalities' null hypotheses but not the specified model (Tanaka, 1987). After reviewing prior research's sample sizes such as Vance et al. (2012) (*n* = 54), Lee et al. (2008) (*n* = 273), (Herath and Rao, 2009) (*n* = 312), and Mohamed and Ahmad (2012) (*n* = 340), it is estimated that this study's sample size would be 250. The sample consists of HE students completing various degrees in a BYOD-enabled Australian university and of diversified demographics.

Stratified sampling method was performed on the respondents' gender by following a 1:1 ratio. This would help to reduce the bias caused by the gender's difference in such a heterogeneous sample and ensure insights from both gender's groups are represented equally (Black, 1999). The data were collected in two modes (i.e. online and in-person) to reduce coverage error. For the online mode, the questionnaire was advertised on Facebook and Twitter and returned 109 responses. For the in-person mode, the researchers invited the students to fill in the questionnaire face-to-face and received 173 responses. As a result of a one-month survey, the researchers obtained 282 responses in total with 30 invalid data, resulting in a sample size of 252 (i.e. usable rate of 89%).

5. DATA ANALYSIS

The hypotheses fall into two groups: (1) measuring impacts (H5–H10) and (2) detecting differences between them across the contexts (H1a–H10a). To measure simultaneously the cognitive process' impacts on intention to perform malware avoidance behaviours, multiple-group structural equation modeling (MSEM) was employed. On the other hand, paired *t*-test (Field, 2009) and revised *z*-test's formula for comparing regression coefficients by Brame et al. (1998) were used to test the differences of effect sizes across the contexts.

5.1. Descriptive analysis

The survey retrieved back 128 male and 124 female responses which are consistent to the stratified proportions. In general, the demographics of the surveyed sample reflected quite accurately the average population of HE students, including a dominant amount of students who are 18–21 years old and completing Bachelor programs. In addition, 22.2% of them belong to the more matured ages range (24 years old and older). Likewise, 15.5% of the surveyed students fell into the categories of Masters and Doctoral degrees, while 16.8% are TAFE (vocational tertiary programs), Diploma and Associate degrees. More important, a majority of their information security skills was self-rated as "intermediate" (48.8%) and some "advanced" (31.0%), whereas the proportions of "beginner" and "expert" users are 9.5% and 10.7% respectively. Consequently, this ratio could reflect the general population of Internet users. Nevertheless, the researchers did not collect data about the students' different cultures which may influence their perceptions; therefore, the self-rated security skill is as the main estimator of information security considerations. Furthermore, it is expected that the students with intermediate or above information security knowledge would understand well the meanings and purposes of the questionnaire's items. On the other hand, the durations of Internet use distributed evenly from 1 to 8 hours per day (84.9%), mostly on Windows laptops and tablets (61.3%), iPhones (27.31%) and Android phones (17.31%). Finally, the purposes of using the Internet matched with the scope of this study which is about non-work activities such as entertainment (20.20%), communication (20.10%), read news and search for information (15.69%). All of the surveyed students were located and approached in-person by the researchers within the BYOD-enabled campus while using their own devices to work on the Internet. The demographics of the sample are summarised in Table 1.

Table 1: Demographics

Ages ranges	%	Programs	%	Information security skills	%
18–19	31.7	TAFE	6.0	Beginner	9.5
20–21	31.3	Diploma	5.6	Intermediate	48.8
22–23	14.7	Associate	5.2	Advanced	31.0
24–25	9.1	Bachelor	67.9	Expert	10.7
26–30	8.3	Masters	12.7		
>30	4.8	PhD	2.8		
Internet uses (hours per day)	%	Mobile devices uses	%	Purposes of Internet uses	%
1–2	20.2	iPhone	27.31	Work	7.94
3–4	27.0	iPad	13.08	Study	21.47
5–6	22.6	Apple laptops	10.96	Entertainment	20.20
7–8	15.1	Android phones	17.31	Online banking	14.12
9–10	6.7	Android tablets	4.42	Communication	20.10
>10	8.3	Windows phones	2.12	Read news and search info	15.69
		Windows tablets	20.00	Other	0.49
		Windows laptops	41.30		
		BlackBerry phones	0.96		
		Other	1.92		

5.2. Paired t-test (H1a–H4a)

By conducting the paired *t*-test (Field, 2009), the researchers sought the statistical significant ($p < 0.05$) differences in the four intentions to perform malware avoidance behaviours so to answer hypotheses H1a–H4a. Specifically, the students' opinions about these intentions were measured in ITA1 (examine sender's address in emails), ITA2 (examine emails' genuine content), ITA3 (avoid clicking on malicious websites) and ITA4 (lock mobile devices). As shown in Table 2, all four intentions to perform malware avoidance behaviours are different across the two contexts at 5% significance level. The *t*-tests are considered robust against violation of normality's assumptions thus the results remained intact and reliable (Boneau, 1960). Given those results, hypotheses H1a, H2a, H3a and H4a were supported.

Table 2: Paired *t*-test results (U=University; H=Home)

Pair		$\Delta\overline{x}$	SD	*r*	*t*	*df*	*p* (2-tailed)	Stronger context
1	ITA1 (U) – ITA1 (H)	-0.198	1.022	-0.194	-3.082	251	0.002	Home
2	ITA2 (U) – ITA2 (H)	-0.238	1.025	-0.232	-3.687	251	0.000	Home
3	ITA3 (U) – ITA3 (H)	-0.341	1.127	-0.303	-4.808	251	0.000	Home
4	ITA4 (U) – ITA4 (H)	0.782	1.746	0.448	7.108	251	0.000	University

5.3. Multiple-group structural equation modeling (Multiple-group SEM)

SEM which combines factor analysis and path analysis to develop and validate conceptual models is well-known in behavioural research field (Hox and Bechger, 1998). As this research's focal interests lie in testing the impacts of contextual difference on the relationships between HE students' cognitive process and their intention to perform malware avoidance behaviours, the use of SEM was justified. To fully develop the PMT conceptual model from the data, the researchers conducted exploratory factor analysis (EFA), multiple-group confirmatory factor analysis (multiple-group CFA) and multiple-group SEM. More specifically, the analysis adhered to the four-step SEM approach guided by (Mulaik and Millsap, 2000) which includes: 1) perform exploratory factor analysis, 2) specify measurement model and 3) structural model, and finally 4) test pre-specified hypotheses. Bayesian structural equation modeling techniques were employed to run simulations and add rigour to step 4th.

The purpose of the EFA process is to explore the patterns of the items from which the common factors can be detected (Brown, 2006). As consistent to PMT's model, the researchers aimed to extract seven factors: intention to perform (ITA), vulnerability (VUL), severity (SEV), rewards (REW), response efficacy (REF), response cost (COS) and self-efficacy (SEF). Principal Axis Factoring was selected as the estimation method since it is free from distributional assumptions (Brown, 2006). Direct Oblimin was used to rotate extracted factors since it offers a more realistic and accurate representation of the interrelated factors (Brown, 2006). The estimated patterns should include items that have loadings exceeding the suggested thresholds of 0.35 (Lewis et al., 2005). As a result, the analysis retained 25 out of 28 items (ITA4, SEF4 and REF4 were removed). The EFA results in KMO = 0.776 and Bartlett's test $p < 0.05$ which indicated factorability is acceptable (Hair et al., 2010). The item loadings of this extraction illustrated in Table A (Appendix) shows that all constructs are valid (i.e. convergent and discriminant validity) and uni-dimensional. Next, each detected factor's measurement model was tested with multiple-group CFA. Construct reliability was assessed using Cronbach's α and coefficient *H*. Since Cronbach's α assumes the models to be essentially τ-equivalent (i.e. equivalent factor loading across indicators) while the measurements are not, coefficient *H* will produce more accurate reliability coefficients (Molla et al., 2011). Table 3 displays all measurement models fit the data and achieve convergent validity and construct reliability.

Table 3: MCFA Convergent Validity Test

Factor	χ^2	*df*	*p*	RMSEA	SRMR	CFI	H_{home}	α_{home}	H_{uni}	α_{uni}
ITA	0.349	3	0.951	0.000	0.0064	1.000	0.84	0.75	0.98	0.82
COS	0.082	2	0.960	0.000	0.0015	1.000	0.92	0.85	0.91	0.85
REF	4.394	6	0.624	0.000	0.0043	1.000	0.88	0.77	0.92	0.87
SEF	1.457	5	0.918	0.000	0.0104	1.000	0.90	0.76	0.91	0.82
REW	2.388	6	0.881	0.000	0.0080	1.000	0.93	0.87	0.93	0.90
VUL	2.031	6	0.917	0.000	0.0109	1.000	0.97	0.88	0.92	0.90
SEV	0.263	3	0.967	0.000	0.0060	1.000	0.92	0.85	0.95	0.85
Criteria	-	-	> 0.050	< 0.060	< 0.070	> 0.960	> 0.70	> 0.70	> 0.70	> 0.70

Based on Fornell and Larcker's criterion (1981), the researchers then calculated average variance extracted (AVE) of each factor and compared it against correlation coefficients estimated from factor scores imputed from the previous step. Tables 4 and 5 show excellent discriminant validity results in two contexts.

Table 4: Discriminant validity tests (home)

Figures in normal font are correlations; in bold are AVEs; in italic are squared correlations

	ITA	COS	REF	REW	SEF	VUL	SEV
ITA	**0.550**	*0.158*	*0.170*	*0.010*	*0.171*	*0.005*	*0.057*
COS	0.397	**0.550**	*0.140*	*0.011*	*0.221*	*0.003*	*0.014*
REF	0.412	0.374	**0.530**	*0.000*	*0.154*	*0.002*	*0.104*
REW	0.099	0.105	0.019	**0.650**	*0.001*	*0.009*	*0.008*
SEF	0.413	0.470	0.392	-0.023	**0.520**	*0.001*	*0.017*
VUL	-0.071	0.053	-0.049	0.096	-0.036	**0.660**	*0.003*
SEV	0.238	0.118	0.322	0.087	0.130	-0.057	**0.620**

Table 5: Discriminant validity tests (university)

	ITA	COS	REF	REW	SEF	VUL	SEV
ITA	**0.640**	*0.198*	*0.157*	*0.021*	*0.201*	*0.005*	*0.055*
COS	0.445	**0.610**	*0.174*	*0.035*	*0.265*	*0.011*	*0.032*
REF	0.396	0.417	**0.660**	*0.020*	*0.193*	*0.002*	*0.106*
REW	0.146	0.186	0.140	**0.700**	*0.000*	*0.013*	*0.002*
SEF	0.448	0.515	0.439	0.003	**0.570**	*0.009*	*0.027*
VUL	0.073	0.107	-0.049	0.116	-0.093	**0.690**	*0.006*
SEV	0.235	0.178	0.326	0.049	0.163	0.079	**0.620**

The researchers subsequently used the factor scores in multiple-group SEM. The original PMT model, however, did not fit with the collected data: $\chi^2(30) = 364.382$ at $p = 0.000$; RMSEA = 0.149; SRMR = 0.1692; CFI = 0.336. Therefore, the model was re-specified and extended (Figure 1) which resulted in excellent fit: $\chi^2(34) = 21.032$ at $p = 0.960$; RMSEA = 0.000; SRMR = 0.0302; CFI = 1.000. It is also worth noticing that the re-specifications also resulted in the extended hypotheses H11–H19 as well as their hypothesised differences H11a–H19a. These extended hypotheses will be discussed later due to the space limit and avoid confusion.

5.4. Bayesian structural equation modeling (Bayesian SEM) (H5–H19; H5a–H19a)

Before concluding with the multiple-group SEM results, Bayesian analysis was performed to overcome the limitations of the sample size ($n = 252$) and the non-normality distributions while adding rigour to such results with their posterior distributions (Lee et al., 2007). This process was conducted using Bayesian SEM function of AMOS software. In contrast with Maximum Likelihood approach, the Bayesian standpoint argues that the true parameters are known and random thus ought to be determined by assigning them probability distributions. Such distributions are called posterior distributions and they can be produced by combining prior ones (i.e. what is already known) and the observed data. As a result, Bayesian analysis summarises the current "state of knowledge" about possible values of parameters, rather than predicting a certain value (Arbuckle, 2010, p. 385). The core process of creating the posterior distributions involves generating samples by using the simulation technique named Markov chain Monte Carlo (MCMC).

In this research, the researchers conducted MCMC simulation by combining non-informative prior distributions and the observed data to create posterior distributions with 304,004 samples. To ensure that each sample is independent from one another, 4 thinning intervals (i.e. 1 out of every 4 samples was kept) were used. The researchers discarded the first 500 burn-in samples and observed 75,501 samples. Each sample has a sample size of 252 observations. At this point the convergence statistic was found to reach the desirable value of 1.0003, whereas value of 1.0000 indicates perfect convergence (Arbuckle, 2010). In other words, the generated results were stable enough for interpretations and the researchers could stop the MCMC procedure. In addition, the estimated parameters had autocorrelation coefficient at near zero by around 20 iterations, suggesting that each distribution has achieved convergence individually and that the randomly-generated data is uncorrelated with the original data. The posterior predictive *p*-value of 0.83 indicates that the model and the randomly-generated data are not statistically different at 5% significance level, meaning that the model holds external validity (Lunza, 1990), although it may slightly underestimate the true values in the population.

Of particular importance is the Bayesian credibility interval (BCI) between which the true value of the parameter resides. Statistical significance with $\alpha = 0.05$ was found to assert that the true values of the estimates would be within the BCIs listed in Table 6. Accordingly, only H5$_{(H)}$, H11, H17$_{(H)}$ and H19 had BCIs include zero values, thus would likely have estimates equal to zero i.e. no impacts in practicality. In contrast, it should be safe to claim that the rest of the hypotheses would have impacts at various magnitudes in real world. In addition, the standard deviations suggested how far the posterior mean values of β deviate from their unknown true values. As seen in Table 6, the overall deviations were small thus ensured the creditability of the findings about the causalities' impacts.

Table 6: Bayesian analysis results

	Hypothesis				95% Bayesian credibility interval of β				SD	
					Lower(H)	Upper(H)	Lower(U)	Upper(U)	H	U
Original PMT Hypotheses	H5	VUL	→	ITA	-0.076	0.001	0.012	0.134	0.015	0.031
	H6	SEV	→	ITA	0.074	0.167	0.069	0.163	0.046	0.046
	H7	REW	→	ITA	0.010	0.109	0.011	0.118	0.031	0.031
	H8	REF	→	ITA	0.119	0.344	0.170	0.227	0.117	0.027
	H9	COS	→	ITA	-0.267	-0.102	-0.248	-0.097	0.046	0.046
	H10	SEF	→	ITA	0.116	0.262	0.257	0.337	0.046	0.027
Extended PMT Hypotheses (due to model re-specifications)	H11	VUL	→	REF	-0.149	0.002	-0.110	0.002	0.015	0.015
	H12	SEV	→	REF	0.249	0.410	0.220	0.375	0.042	0.042
	H13	REF	→	SEF	0.322	0.465	0.364	0.515	0.064	0.064
	H14	REF	→	REW	0.007	0.078	0.080	0.187	0.031	0.046
	H15	REF	→	COS	-0.250	-0.176	-0.295	-0.193	0.040	0.04
	H16	SEF	→	COS	-0.411	-0.301	-0.495	-0.325	0.040	0.054
	H17	VUL	→	COS	-0.084	0.001	-0.235	-0.042	0.015	0.041
	H18	REW	→	COS	-0.176	-0.042	-0.202	-0.048	0.037	0.037
	H19	SEV	→	COS	-0.072	0.030	-0.035	0.001	0.093	0.015

Performing Bayesian SEM also produced the standardised regression coefficients β values and their respective significance level. Table 7 summarised findings of the hypotheses (original and extended due to model re-specifications) in both contexts. As shown, some hypotheses were only supported in one context but not in another while some achieved statistical significance in both contexts (H6, H8, H9 and H10). Interpretations of those hypotheses will be discussed shortly.

Table 7: Bayesian analysis results of regression effects

	Hypothesis				Bayesian's β		*p*-value		Supported?	
					Home	Uni	Home	Uni	Home	Uni
Original PMT Hypotheses	H5	VUL	→	ITA	-0.037	0.074	0.064	0.021	No	Yes
	H6	SEV	→	ITA	0.120	0.115	0.000	0.000	Yes	Yes
	H7	REW	→	ITA	0.060	0.064	0.021	0.021	No	No
	H8	REF	→	ITA	0.234	0.197	0.000	0.000	Yes	Yes
	H9	COS	→	ITA	-0.186	-0.175	0.000	0.000	Yes	Yes
	H10	SEF	→	ITA	0.190	0.296	0.000	0.000	Yes	Yes
Extended PMT Hypotheses (due to model re-specifications)	H11	VUL	→	REF	-0.073	-0.054	0.064	0.064	No	No
	H12	SEV	→	REF	0.330	0.296	0.000	0.000	Yes	Yes
	H13	REF	→	SEF	0.395	0.442	0.000	0.000	Yes	Yes
	H14	REF	→	REW	0.043	0.133	0.021	0.000	Yes	Yes
	H15	REF	→	COS	-0.214	-0.243	0.000	0.000	Yes	Yes
	H16	SEF	→	COS	-0.358	-0.414	0.000	0.000	Yes	Yes
	H17	VUL	→	COS	-0.041	-0.140	0.064	0.005	No	Yes
	H18	REW	→	COS	-0.110	-0.126	0.001	0.001	No	No
	H19	SEV	→	COS	-0.021	-0.017	0.902	0.064	No	No

Finally, given the regression coefficients β in both contexts resulting from the Bayesian SEM process, the researchers proceeded on detecting the statistical significant differences among those coefficients. This helps to answer hypotheses H5a–H10a (as well as H11a–H19a) and ultimately research question 2. Specifically, the researchers employed the revised z-test formula by Brame et al. (1998) which was suggested to correctly compare the regression coefficients' differences without the downward bias of their standard deviation. The corrected formula is written as below.

$$z = \frac{b_1 - b_2}{\sqrt{SE^2_{(b_1)} + SE^2_{(b_2)}}}$$

The difference between the effect sizes across the contexts is considered statistically significant if its calculated *z*-score is larger than the common thresholds of 1.96 or -1.96 (Field, 2009). Table 8 summarised the figures required for the computations as well as their results. As displayed, only H5a (*z*-score = 3.223), H10a (*z*-score = 1.987) and H17a (*z*-score = -2.268) were confirmed to have statistical significant differences at *p*-value lower than 0.05.

Table 8: z-test results for detecting differences in regression effects

	Hypothesis				S.E. Home	 Uni	Δβ	z-score	Supported?
Original PMT Hypotheses	H5a	VUL	→	ITA	0.015	0.031	0.111	3.223	Yes
	H6a	SEV	→	ITA	0.046	0.046	0.005	-0.077	No
	H7a	REW	→	ITA	0.031	0.031	0.004	0.091	No
	H8a	REF	→	ITA	0.117	0.027	0.037	-0.308	No
	H9a	COS	→	ITA	0.046	0.046	0.011	0.169	No
	H10a	SEF	→	ITA	0.046	0.027	0.106	1.987	Yes
Extended PMT Hypotheses (due to model re-specifications)	H11a	VUL	→	REF	0.015	0.015	0.019	0.896	No
	H12a	SEV	→	REF	0.042	0.042	0.034	-0.572	No
	H13a	REF	→	SEF	0.064	0.064	0.047	0.519	No
	H14a	REF	→	REW	0.031	0.046	0.090	1.622	No
	H15a	REF	→	COS	0.040	0.04	0.029	-0.513	No
	H16a	SEF	→	COS	0.040	0.054	0.056	-0.833	No
	H17a	VUL	→	COS	0.015	0.041	0.099	-2.268	Yes
	H18a	REW	→	COS	0.037	0.037	0.016	-0.306	No
	H19a	SEV	→	COS	0.093	0.015	0.004	0.042	No

6. RESULTS & DISCUSSIONS

6.1. RQ1 (H1a–H4a): Do intentions to perform malware avoidance behaviours differ across contexts?

From the paired *t*-tests, all hypothesised differences among the four intentions to perform malware avoidance behaviours (H1a–H4a) were supported at significance threshold ($p < 0.05$). To interpret the magnitudes of those differences across the contexts, the researchers employed Faul et al.'s G*Power 3.1 software (2007) to calculate their effect size. These effect sizes were displayed in Table 2 as *r*.

Accordingly, the HE students' intentions to carefully examine email's content and sender's address differed in small effect sizes (r_{ITA1} = -0.194 and r_{ITA2} = -0.232). As a result, it is suggested that the students intended to perform the same safe behaviours when checking emails both at home and at university. In contrast, avoiding malicious websites and locking devices achieved medium magnitudes of differences (r_{ITA3} = -0.303 and r_{ITA4} = 0.448) across the contexts. This could be interpreted that the students were keener on detecting malicious URLs at home while intended to lock their devices more at university.

Revision of Li and Siponen's hypotheses (2011) about contextual differences hinted that the students' awareness about their insecure home network has motivated them to be more cautious at home, thereby performing malware avoidance behaviours more actively. This resulted in the stronger intention to avoid clicking malicious websites at home. In addition, it was reasonable that the students would lock their devices more often at university due to high risks of thief or loss. On the other hand, the small differences in carefully examining emails may reflect that performing such behaviours has become a routine task of the HE students, therefore their intentions did not differ much across the contexts.

6.2. RQ2 (H5–H19; H5a–H19a): To what extent the cognitive process's impacts on intention to perform changed across the contexts?

6.2.1. Original Protection Motivation Theory hypotheses (H5–H10; H5a–H10a)

Applying the revised *z*-test formula by Brame et al. (1998) on the Bayesian SEM's results answered research question 2. In overall, three statistically significant differences (H5a, H10a and H17a) were found in the cognitive process's impacts on the students' intention to perform malware avoidance behaviours. The researchers discussed the findings of hypotheses H5–H19 (as well as H5a–H19a respectively) as follow.

First, perception of *vulnerability* only achieved statistical significance when positively impacting the students' intention to perform malware avoidance behaviours at university ($\beta_{ITA,VUL} = 0.074$). This result was consistent with similar studies such as Lee et al. (2008), albeit demonstrated weaker effect. Interestingly, the non-significant negative impact of vulnerability when perceived at home mirrored Vance et al.'s result (2012). Accordingly, Vance et al. (2012) found the employee's perception of vulnerability did not affect their compliance intention ($\beta = 0.10$; $p > 0.05$). This study also detected a small change ($\Delta\beta_{ITA,VUL} = 0.111$) in how perceived vulnerability drove the students' intention to perform malware avoidance behaviours. Specifically, they were more motivated to perform secured non-work activities when at university. One explanation was that they felt more vulnerable against malware at university, which contradicted the researchers' anticipation. Another possible reason is that the construct vulnerability may have various meanings that were perceived differently by the students according to the contexts.

Second, the finding supported H6 in both contexts, therefore suggested *severity* as an effective predictor of intention to perform malware avoidance behaviours. Again, this study's results ($\beta_H = 0.120$; $\beta_U = 0.115$) were weaker than finding of Vance et al.'s (2012) about compliance ($\beta = 0.270$). On the other hand, Lee et al. (2008) detected smaller impact of severity on virus protection behaviour ($\beta = 0.037$; $p > 0.10$). Nevertheless, the researchers found no significant differences in severity's impacts across the two contexts. It could be due to the students may have overlooked the malware's damages on the public resources and assessed the infection's severity solely based on their own devices. In that case, the user's responsibility over the community's online safety should be investigated separately.

Third, the finding failed to support H7 while contradicting both the original PMT and Vance et al.'s study (2012). Specifically, the perceived *rewards* of not performing malware avoidance behaviours were found to motivate such intention to the students. However, the effects in both contexts were trivial in practicality ($\beta_H = 0.060$; $\beta_U = 0.064$). In addition, no significant difference was detected across the contexts. A possible conjecture to explain this unusual outcome was that the students had no choice but to perform the behaviours, albeit realising the rewards of not doing so. Moreover, it may be consistent with the unique characteristics of the sample and should be considered only in Australian HE sector.

Fourth, H8 was supported in both contexts, indicating that the students intended to perform malware avoidance behaviours more as they found them effective. More important, the impacts were stronger ($\beta_H = 0.234$; $\beta_U = 0.197$) than Lee et al.'s (2008) research about installing anti-virus software ($\beta = 0.140$). The findings also contradicted the research of Vance et al. (2012) about compliance ($\beta = -0.21$). Nevertheless, no significant difference was found, therefore suggested that the students perceived the same effectiveness of network security in both contexts. Given this, it is questioned whether the university might have failed to make the students realise the professional security protection.

Fifth, H9 was also confirmed across the contexts. The medium negative magnitudes ($\beta_H = -0.186$; $\beta_U = -0.175$) of *response cost* suggested that the students felt reluctant to perform malware avoidance behaviours as they are perceived inconvenient. The findings were consistent with Vance et al. (2012) which found relative effect size ($\beta = -0.18$). In addition, this negative impact remained stable across the contexts. Controversial conjectures were drawn from this finding. The students may have provided unchanged opinions about the response cost since the questionnaire asked the same behaviours across the contexts. On the other hand, it could be due to the professional security (e.g. firewall, spam filters) that could not reduce the perceived inconveniences.

Sixth, the findings confirmed the last original hypothesis H10 and suggested *self-efficacy* as an effective predictor (β_H = 0.190; β_U = 0.296) of intention to perform malware avoidance behaviours. It is worth noticing that these findings displayed weaker impacts than Lee et al. (2008) (β = 0.504) and Vance et al. (2012) (β = 0.34). More important, a statistically significant small difference ($\Delta\beta_{ITA,SEF}$ = 0.106) was detected. In fact, the students felt more confident in performing malware avoidance behaviours at university than at home.

6.2.2. Extended model re-specifications' hypotheses (H11–H19; H11a–H19a)

By re-specifying the conceptual model to achieve excellent fit, the researchers extended the PMT model and added the additional hypotheses H11–H19 describing the relationships between the cognitive factors. As a result, they helped to understand in-depth the cognitive process and produced complementing results.

First, it was hypothesised that the students would put more expectations in the malware avoidance behaviours to be effective as they felt more vulnerable against the malware threats. Nevertheless, the findings suggested that *vulnerability* failed to increase *response efficacy*, given the non-significant *p*-values (p_H = 0.064; p_U = 0.064).

Second, the researchers had similar expectation about the potential positive effect of *severity* on *response efficacy*. Interestingly, the results confirmed H12 as they showed that perceptions of the behaviours' effectiveness were moderately increased by the students' perceived severity (β_H = 0.330; β_U = 0.296). In addition, the researchers detected no statistically significant change thus suggested *severity* as a stable, effective predictor of *response efficacy*.

Third, it was argued that *response efficacy* was also perceived according to their usability. Therefore, it could be reasonably anticipated that the more they are perceived to be easily performed, the better they could boost the students' *self-efficacy*. Such anticipation was confirmed with medium magnitudes (β_H = 0.395; β_U = 0.442). Again, no statistically significant change across the contexts indicated those positive impacts to remain stable.

Fourth, *rewards* was found in another strange yet confirmed relationship in which it received positive impact from *response efficacy* (β_H = 0.043; β_U = 0.133). A possible conjecture was that the students found the malware avoidance behaviours effective but not be convenient enough to overcome the trade-off costs (i.e. rewards). Moreover, no significant difference was detected.

Fifth, the researchers extended to the hypothesis that the students perceived less *response cost* as they realised more *response efficacy*. Consequently, this hypothesis (H15) was confirmed with medium magnitudes (β_H = -0.214; β_U = -0.243). In addition, this desirable causality was also proven as stable since the researchers detected no change across the contexts.

Sixth, *self-efficacy* could reduce *response cost* with medium effect sizes (β_H = -0.358; β_U = -0.414). Indeed, H16 was confirmed that the students' self-belief in own ability played significant role in convincing them to perform the malware avoidance behaviours. Again, no significant change indicated high stability of this relationship.

Seventh, the third and last difference was confirmed in how *vulnerability* could reduce *response cost*, especially at university (p_H = 0.064; p_U = 0.005). However, the size of this diminishing effect was trivial in practicality (β_U = -0.140), as well as the difference's magnitude ($\Delta\beta_{COS,VUL}$ = 0.099).

Eighth, H18 was not supported albeit achieved statistically significant *p*-values (p_H = 0.001; p_U = 0.001). It was initially expected that the behaviours' *response cost* would be increased as the students realised more the rewards of not performing those behaviours. However, the outcomes suggested that *rewards* decreased *response cost* instead (β_H = -0.110; β_U = -0.126). In other words, the students had no choice but to convince themselves that the behaviours would not be much inconvenient, despite they could have realised the rewards.

Finally, H19's results disconfirmed (p_H = 0.902; p_U = 0.064) the initial anticipation that the students would perceive less *response cost* as they realised the *severity* of being infected by malware. The summary of all hypotheses about the impacts and their differences is illustrated in Figure 1 below.

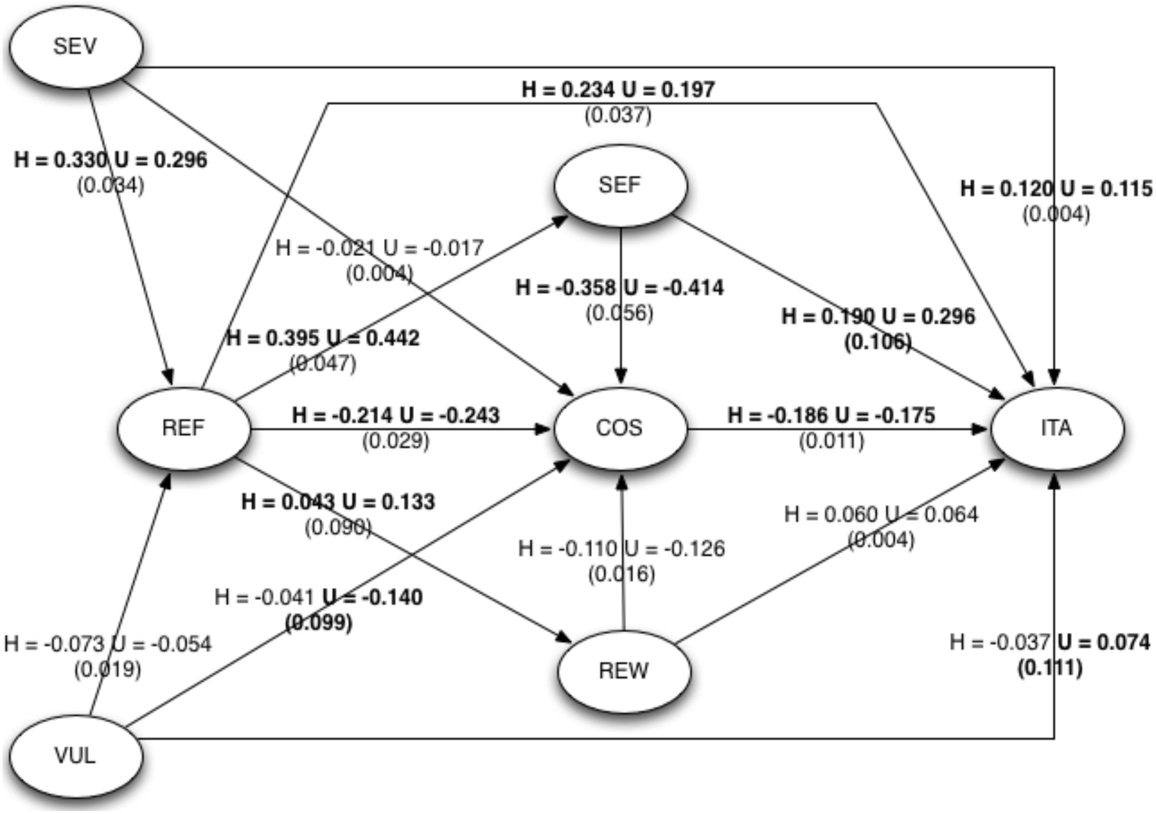

Figure 1: Extended Protection Motivation Theory model (figures in brackets are Δβ differences; bold texts are statistically significant results)

7. RESEARCH IMPLICATIONS

7.1. Implications for practice

The empirical findings of this research provide implications for practice in two ways. Specifically, they illustrated the differences in how mobile devices' owners perceived information security and intended to avoid malware across two contexts, as well as suggested preliminary guidance to design security programs and measures that could balance these differences. Moreover, these findings are especially useful for education institutes that are considering or currently adopting BYOD practices, be it either enforced use of personal mobile devices in classrooms such as the university in this study or voluntarily like EDUROAM. Of particular interest are the different perceptions of *self-efficacy* and *vulnerability*'s impacts towards intention to perform malware avoidance behaviours (and *vulnerability* towards *response cost*). While these constructs have been consistently found by various studies to influence intention to perform information security behaviours, little attention is paid on their nature.

As mentioned above, the students perceived their self-efficacy to be a stronger motivation for performing malware avoidance behaviours at university than at home. In other words, it is supported empirically that individual's reliance on their own *self-efficacy* is inconstant. This variance is viewed as both a challenge and opportunity to be considered by information security management. First, a person possessing a certain level of information security skills may hesitate to trust their ability to perform malware avoidance behaviours when being in the same situations (e.g. browsing emails or websites) but of different contexts. This alerts management about the reluctance of the users towards their own skills and the difficulties that they have to face when making security decisions, even to the advanced users. More important, it emphasises that information security training must not be a one-off attempt.

At the same time, the inconstant influence of perceived *self-efficacy* suggests an opportunity that it could be malleable and improved. Consider that the students in this study would be more independent at home, whereas the university context offers professional technical supports and informal helps from peers, the researchers contended that the changing impact of *self-efficacy* could be a group phenomenon. If that was the case, it highlights the important roles of the available supports (informal and formal) in boosting the confidence of individuals to avoid malware threats by relying on their ability. Organisations are suggested to develop a community of practice to assist with information security matters, especially to encourage continuous assistance among the users to enhance perceptions about *self-efficacy*'s effectiveness and foster security climate and culture in long term. Furthermore, training programs should be designed in series to include reflections and revisions to boost the users' confidence in applying the learned techniques. Otherwise, the acquired knowledge is ineffective and costly if the users feel reluctant to use it.

Perceived *vulnerability* also has an interesting variance of effects across contexts and implies practical values. Accordingly, the students only found their vulnerability as a motivation to avoid malware threats when they were at university. In other words, the students may or may not feel the malware threats while using mobile devices at home, but either way they were never considered the reason for performing the security behaviours. This finding could also have two different interpretations. First, it should be noted that perceived *severity* was found to impact intention to avoid malware. By considering these two motivations of intention, it could be argued that the threats were taken as a given, and because of that the students would be concerned more by the consequences of the threats to take actions. On the other hand, perceiving vulnerability at public place but not at home may signify ignorance of risks if the students believed that malware threats only exist when their devices are physically exposed, or household's information security is not worthy for potential attacks. While the first interpretation could be valuable to designing security messages that focus on the severity of threats to motivate home users' security actions, the second indicates a weak security state at home that needs to be improved.

The previous paragraphs have discussed much on the practical meanings of how users at home and at public place such as university perceived differently the impacts on intention to avoid malware. The coming discussions will elaborate how security programs, measures or messages could be designed to improve the situations. To begin with, it is imperative to improve the security practices, for the construct *response efficacy* has been consistently found to motivate intention to perform security behaviours. More specifically, the supported hypotheses in this study highlighted that the usability of these practices also plays an important role besides their perceived efficacy, since the extended hypothesis H13 has shown that *response efficacy* could lead to higher perceived *self-efficacy*. In other words, the better practices should help the users to raise their confidence in tackling the security problems. Furthermore, *response efficacy* could also reduce perceived *response cost*, which is a significant obstacle that demotivates the users' intention to avoid malware. Finally, to make the users believe more in the practices' effectiveness, this research suggests practitioners to put emphasis on the *severity* of the threats rather than the *vulnerability* of the users or the organisation's systems, at least for contexts that are similar to the one in this study. For instance, instead of designing the message that states "carelessly downloading attachments from any emails would result in malware infection" (i.e. vulnerability-focused), a message with stronger impact would be "malware infection caused by attachments from emails is a serious problem (to us) that could destroy series of data, loss of productivity and may be impossible to recover". By doing this way, the researchers expect the threats to be taken as a given, and the users or organisations could be put in the state of constant awareness.

7.2. Implications for research

The empirical findings provided theoretical implications that could be considered by future research. First, Protection Motivation Theory was again supported by this study to be consistently capable of determining the antecedents of intention to perform information security behaviours. More important, in this particular context that requires the users to proactively avoid malware threats in an environment that demands less commitment and responsibility, the PMT model was specified and extended as shown in Figure 1. This extended version of the model is argued to reflect the user's cognition in such specific context and the researchers suggest future studies to further test the model's viability. With the growing adoption of BYOD and personal mobile devices in different contexts–from corporate environments to public places–it would be useful in the near future to apply this PMT model in situations where the "Comply or Die" approach becomes less effective and proactive protection of security-aware agents is necessary (Kirlappos et al., 2014, 2013).

Nonetheless, this study would be only considered as the first milestone to advance into the domain of BYOD-related information security behaviours. To assist future studies' endeavours, the researchers have demonstrated step-by-step in details the appropriate quantitative methods that could be used to measure and compare empirical findings across different contexts. Specifically, further investigations are suggested to explore the other pairs of contexts that involve work-activities. In addition, identifying the contextual factors and their effects on the changes of intention to perform (Li and Siponen, 2011) is an important research direction that would bring interesting results. For instance, was it due to the different levels of responsibility or something else that made the users perceived different weights of the factors' contributing effects to malware avoidance intention in two contexts? Gaining more understanding about such contextual factors would be crucial in designing security programs and measures that balance the differences between contexts. Moreover, the constructs *vulnerability* was hypothesised to have different meanings according to the contexts. Future studies are recommended to explore these contextual meanings as they may produce important insights.

8. LIMITATIONS

While the researchers have performed rigourous data analyses to their best, it was inevitable for this research to have some limitations. First, the sample consisted of HE students, albeit of diversified demographics, could not represent the population of Internet users and their changes in the intention to perform malware avoidance behaviours. Second, given the examined contexts, these results would be most applicable in educational sector but not in any BYOD environments. It was also worth noticing that only two out of four contexts suggested by Li and Siponen (2011) were investigated in this research.

9. CONCLUSION

The analyses and findings shed light on Li and Siponen's proposed issues (2011) of changing information security behaviours across contexts. Specifically, the research supported that carefully browsing emails and websites received stronger intention at home as compared with locking mobile devices at public place, especially when the students performed non-work Internet activities. The Protection Motivation Theory-based model with extended hypotheses further explained how the cognitive factors impacted such intention, and more important, how these factors changed their effects from one context to another.

The findings altogether emphasised the extant cyber-threats in the user's changing intention to perform malware avoidance behaviours. In other words, academics and practitioners are recommended to raise awareness about the fact that users are not always willing to carefully avoid malware, even when they are performing the same non-work activities on the Internet. On the other hand, the extended conceptual model provided directions to enhance information security trainings' effectiveness, particularly about the user's ability to avoid malware threats by exploiting the cognitive effects. Moreover, suggestions for future research were also included. Ultimately, this research serves as one of the first milestones to address the emerging cyber-threats associated with the trending BYOD adoption in global organisations, especially in the education sector.

REFERENCES

ACMA, 2013. Communications report 2011–12 series, Report 3–Smartphones and tablets, Take-up and use in. Canberra.

Adhikari, J., Parsons, D., Mathrani, A., 2006. Bridging Digital Divides in the Learning Process: Challenges and Implications of Integrating ICTs. pp. 1–4.

Allam, S., Flowerday, S. V., Flowerday, E., 2014. Smartphone information security awareness: A victim of operational pressures. Comput. Secur. 42, 56–65.

Anderson, C.L., Agarwal, R., 2010. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions. MIS Q. 34, 613–643.

Arbuckle, J.L., 2010. IBM SPSS Amos 19 User's Guide. Amos Development Corporation.

AusCERT, 2008. Home Users Computer Security Survey 2008. Brisbane, Australia.

Australian Government, 2014. Bring Your Own Device (BYOD) Considerations for Executives.

Barkhuus, L., 2005. “Bring Your Own Laptop Unless You Want to Follow the Lecture”: Alternative Communication in the Classroom. In: Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work. ACM, 2005. pp. 140–143.

Bidin, S., Ziden, A.A., 2013. Adoption and Application of Mobile Learning in the Education Industry. Procedia - Soc. Behav. Sci. 90, 720–729.

Black, T.R., 1999. Doing quantitative research in the social sciences: An integrated approach to research design, measurement, and statistics. Thousand Oaks, CA: SAGE Publications, Inc.

Boer, H., Seydel, E.R., Norman, P., 1996. Protection motivation theory. Predict. Heal. Behav. Res. Pract. with Soc. Cogn. Model. 95–120.

Boneau, A.C., 1960. The effects of violations of assumptions underlying the t test. Psychol. Bull. 57, 49–64.

Brame, R., Mazerolle, P., Piquero, A., 1998. Using The Correct Statistical Test For The Equality Of Regression Coefficients. Criminology 36, 859–866.

Brown, T.A., 2006. Confirmatory Factor Analysis for Applied Research. The Guilford Press.

Burt, J., 2011. BYOD Trend Pressures Corporate Networks. eWeek 28, 30–32.

Centre for Internet Safety, 2011. Password Security–a Survey of Australian Attitudes Toward Password Use and Management. Canberra.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101.

Emery, S., 2012. Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education.

Faul, F., Erdfelder, E., Lang, A.-G., Buchner, A., 2007. G*Power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behav. Res. Methods 39, 175–91.

Field, A., 2009. Discovering Statistics using SPSS. Sage Publications Ltd.

Fornell, C., Larcker, D.F., 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Mark. Res. 18, 39–50.

Gajar, P.K., Ghosh, A., Rai, S., 2013. BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES. J. Glob. Res. Comput. Sci. 4, 62–70.

Google, 2013. Good To Know - A guide to staying safe and secure online [WWW Document]. URL http://www.google.com/goodtoknow/online-safety/locking/

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2010. Multivariate Data Analysis, 7th ed, Multivariate data analysis. Prentice Hall, Upper Saddle River, NJ.

Hamza, A., Noordin, M.F., 2013. BYOD Usage by Postgraduate Students of International Islamic University Malaysia: An Analysis. Int. J. Eng. Sci. Invent. 2, 14–20.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125.

Hox, J.J., Bechger, T.M., 1998. An Introduction to Structural Equation Modeling. Fam. Sci. Rev. 11, 354–373.

Internet World Stats, 2014. Internet Usage and Population in Oceania [WWW Document]. URL http://www.internetworldstats.com/stats6.htm

Jain, A.K., Shanbhag, D., 2012. Addressing Security and Privacy Risks in Mobile Applications. IT Prof. 28–33.

Johnston, A.C., Warkentin, M., 2010. Fear Appeals And Information Security Behaviors: An Empirical Study. MIS Q. 34, 549–566.

Kirlappos, I., Beautement, A., Sasse, M.A., 2013. “Comply or Die” Is Dead: Long Live Security-Aware Principal Agents The Need for Information Security. In: Financial Cryptography and Data Security. Springer Berlin Heidelberg, pp. 70–82.

Kirlappos, I., Parkin, S., Sasse, M.A., 2014. Learning from “Shadow Security”: Why understanding non-compliant behaviors provides the basis for effective security.

Kline, R.B., 2011. Principles and Practice of Structural Equation Modeling, 3rd ed. Guilford Press, New York, NY, USA.

Kobus, M.B.W., Rietveld, P., van Ommeren, J.N., 2013. Ownership versus on-campus use of mobile IT devices by university students. Comput. Educ. 68, 29–41.

Lee, D., Larose, R., Rifon, N., 2008. Keeping our network safe: a model of online protection behaviour. Behav. Inf. Technol. 27, 445–454.

Lee, S.-Y., Song, X.-Y., Tang, N.-S., 2007. Bayesian Methods for Analyzing Structural Equation Models With Covariates, Interaction, and Quadratic Latent Variables. Struct. Equ. Model. A Multidiscip. J. 14, 404–434.

Lee, Y., Kozar, K. a., 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. Inf. Manag. 45, 109–119.

Lennon, R., 2012. Changing user attitudes to security in bring your own device (BYOD) & the cloud. In: Tier 2 Federation Grid, Cloud & High Performance Computing Science (RO-LCG), 2012 5th Romania. pp. 49–52.

Lewis, B.R., Templeton, G.F., Byrd, T.A., 2005. A methodology for construct development in MIS research. Eur. J. Inf. Syst. 14, 388–400.

Li, Y., Siponen, M., 2011. A Call for Research on Home Users' Information Security Behaviour. In: 15th Pacific Asia Conference on Information Systems (PACIS).

Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11, 394–413.

Lunza, M.L., 1990. A Methodological Approach to Enhance External Validity in Simulation Based Research. Issues Ment. Health Nurs. 11, 407–422.

Luszczynska, A., Schwarzer, R., 2005. Social cognitive theory. Predict. Heal. Behav. 2 2, 127–169.

Mansfield-Devine, S., 2012. Interview: BYOD and the enterprise network. Comput. Fraud Secur. 2012, 14–17.

Markelj, B., Bernik, I., 2012. Mobile Devices and Corporate Data Security. Int. J. Educ. Inf. Technol. 6, 97–104.

Miller, K.W., Voas, J., Hurlburt, G.F., 2012. BYOD: Security and Privacy Considerations. IT Prof. 53–55.

Mohamed, N., Ahmad, I.H., 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Comput. Human Behav. 28, 2366–2375.

Molla, A., Cooper, V., Pittayachawan, S., 2011. The Green IT Readiness (G-readiness) of Organisations: An Exploratory Analysis of a Construct and Instrument. Commun. Assoc. Inf. Syst. 29.

Mulaik, S., Millsap, R., 2000. Doing the four-step right. Struct. Equ. Model. A Multidiscip. J. 7, 36–73.

Ng, B., Rahim, M., 2005. A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. In: PACIS. pp. 234–247.

Northern Grampians Council, 2013. ICT Strategy 2013-2017. Victoria.

NSW Government, 2014. Student Bring Your Own Device Policy (BYOD) [WWW Document]. URL https://www.det.nsw.edu.au/policies/technology/computers/mobile-device/PD20130458.shtml

Nykvist, S., 2012. The trials and tribulations of a BYOD science classroom. In: Proceedings of the 2nd International STEM in Education Conference. pp. 331–334.

Office of the Information Commissioner Queensland, 2014. Use of portable storage devices. Queensland.

Ponemon Institute, 2012. 2011 Cost of Data Breach Study: Global. Traverse City, Michigan, USA.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 93–114.

Romer, H., 2014. Best practices for BYOD security. Comput. Fraud Secur. 2014, 13–15.

Samochadin, A., Raychuk, D., Voinov, N., Ivanchenko, D., Khmelkov, I., 2014. MDM based Mobile Services in Universities. In: International Conference on Emerging of Networking, Communication and Computing Technologies (ICENCCT 2014). pp. 35–41.

Silic, M., Back, A., 2014. Shadow IT – A view from behind the curtain. Comput. Secur. 45, 274–283.

Siponen, M., Pahnila, S., Mahmood, A., 2007. Employees' adherence to information security policies: an empirical study. New Approaches Secur. Priv. Trust Complex Environ. 232, 133–144.

Sophos, 2014. Security Threat Report 2014.

Spafford, E.H., 2013. Editorial. Comput. Secur. 32, v.

Symantec, 2013. INTERNET SECURITY THREAT REPORT 2013. Moutain View, USA.

Tanaka, J.S., 1987. "How Big Is Big Enough?": Sample Size and Goodness of Fit in Structural Equation Models with Latent Variables. Child Dev. 58, 134–146.

Thomson, G., 2012. BYOD: enabling the chaos. Netw. Secur. 2012, 5–8.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Inf. Manag. 49, 190–198.

Vesey, P.E., 2013. Students' Voice on Mobile Technology and Web 2.0 Tools for Learning. The Universtiy of Waikato.

Willison, R., Warkentin, M., 2013. Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Q. 37, 1–20.

APPENDIX

Table A: Questionnaire's measures and EFA results

Construct	Measure	Reliability (α)		Item loading	Question	Source(s)	Refined question
		H	U				
Intention to perform malware avoidance behaviours	ITA1	0.75	0.82	-0.788	How likely would you be to perform the following actions: Carefully examine whether the received email is from the genuine sender.	Herath and Rao (2009)	When at HOME/UNIVERSITY, how likely would you be to perform the following actions: Carefully examine whether the received email is from the genuine sender.
	ITA2			-0.791	How likely would you be to perform the following actions: Carefully examine whether the received email has suspicious links or attachments, even when it comes from someone you know.	Herath and Rao (2009)	When at HOME/UNIVERSITY, how likely would you be to perform the following actions: Carefully examine whether the received email has suspicious links or attachments, even when it comes from someone you know.
	ITA3			-0.430	How likely would you be to perform the following actions: Avoid clicking on suspicious websites or advertisements that appear to be scams.	Herath and Rao (2009)	When at HOME/UNIVERSITY, how likely would you be to perform the following actions: Avoid clicking on suspicious websites or advertisements that appear to be scams.
Vulnerability	VUL1	0.88	0.90	0.648	I could be targeted to a malware injection.	New	I could be targeted to a malware injection.
	VUL2			0.854	The computer I'm using can be easily infected with malware.	New	The computer I'm using can be easily infected with malware.
	VUL3			0.946	There is a good chance that my computer could be infected by malware.	Johnston and Warkentin (2010)	There is a good chance that my computer could be infected by malware.
	VUL4			0.799	It is likely that I could already have malware.	New`	It is likely that I could already have malware.
Severity	SEV1	0.85	0.85	0.565	I believe that being infected by malware is a serious problem to me.	Johnston and Warkentin (2010); Vance et al. (2012)	I believe that being infected by malware is a serious problem to me.
	SEV2			0.846	I believe that the time loss to recover the damages (e.g., data loss, malfunctioning computer) from being infected by malware is a serious problem	New	I believe that the time loss to recover the damages (e.g., data loss, malfunctioning computer) from being infected by malware is a serious problem
	SEV3			0.902	I believe that the productivity loss to recover the damages (e.g., data loss, malfunctioning computer) from being infected by malware is a serious problem	Herath and Rao (2009)	I believe that the productivity loss to recover the damages (e.g., data loss, malfunctioning computer) from being infected by malware is a serious problem
	SEV4			0.807	I believe that the data/information loss from being infected by malware is a serious problem	Herath and Rao (2009)	I believe that the data/information loss from being infected by malware is a serious problem
Rewards	REW1	0.87	0.90	-0.922	Not performing any of the provided recommendations helps me to finish my tasks quickly	Vance et al. (2012)	Not performing (1) helps me to finish my tasks quickly
	REW2			-0.877	Not performing any of the	New	Not performing (2) helps me to finish

					provided recommendations simplifies my steps to use the computer		my tasks quickly
	REW3			-0.834	Not performing any of the provided recommendations requires me less effort	New	Not performing (3) helps me to finish my tasks quickly
	REW4			-0.596	Not performing any of the provided recommendations makes me feel less stressful	New	Not performing (4) helps me to finish my tasks quickly
Response Efficacy	REF1	0.77	0.87	0.773	Performing any of the provided recommendations would reduce the chance my computer would be infected with a malware	Lee et al. (2008); Mohamed and Ahmad (2012); Vance et al. (2012)	Performing (1) would reduce the chance my computer would be infected with a malware
	REF2			0.785	Performing any of the provided recommendations prevents malware from infecting my computer	Lee et al. (2008)	Performing (2) would reduce the chance my computer would be infected with a malware
	REF3			0.782	Performing any of the provided recommendations makes me feel safe when using my computer	New	Performing (3) would reduce the chance my computer would be infected with a malware
Self-efficacy	SEF1	0.76	0.82	0.813	I feel confident when performing either of the provided recommendations	Lee et al. (2008)	I perform (1) easily
	SEF2			0.918	I perform any of the provided recommendations without being instructed	Herath and Rao (2009); Vance et al. (2012)	I perform (2) easily
	SEF3			0.539	I perform either of the provided recommendations easily	Herath and Rao (2009); Mohamed and Ahmad (2012); Vance et al. (2012)	I perform (3) easily
Response Cost	COS1	0.85	0.85	-0.735	Performing either of the provided recommendations creates more hindrances to me	Herath and Rao (2009); Vance et al. (2012)	Performing (1) is inconvenient
	COS2			-0.783	Performing any of the provided recommendations costs me time	New	Performing (2) is inconvenient
	COS3			-0.675	Performing any of the provided recommendations costs me extra effort	Vance et al. (2012)	Performing (3) is inconvenient
	COS4			-0.572	Performing any of the provided recommendations complicates my task	New	Performing (4) is inconvenient
Criteria	-	>0.70	>0.70	>±0.35	-	-	-