2013

# Contextual Difference and Intention to Perform Information Security Behaviours Against Malware in a BYOD Environment: a Protection Motivation Theory Approach

Duy Pham Thien Dang
*RMIT University*, duy.dangphamthien@rmit.edu.vn

Siddhi Pittayachawan
*RMIT University*, siddhi.pittayachawan@rmit.edu.au

Mathews Zanda Nkhoma
*RMIT University*, mathews.nkhoma@rmit.edu.vn


# Information Systems: Transforming the Future

## 24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

## Proudly sponsored by


ACIS 2013 Principal Sponsor







# Contextual Difference and Intention to Perform Information Security Behaviours Against Malware in a BYOD Environment: a Protection Motivation Theory Approach

Duy P.T. Dang, Siddhi Pittayachawan
School of Business IT and Logistics
RMIT University
Melbourne, Australia
Email: duy.dangphamthien@rmit.edu.vn, siddhi.pittayachawan@rmit.edu.au

Mathews Z. Nkhoma
Business IT and Logistics Department
RMIT University Vietnam
Ho Chi Minh City, Vietnam
Email: mathews.nkhoma@rmit.edu.vn

**Abstract**

*The research domain of end-user's information security behaviours has been gaining much attention over the recent years. While the nature of intention to perform information security behaviours are being revealed, there are still gaps in this area. In particular, few studies have addressed whether such intention remains across contexts, especially from home to public places. Secondly, the amount of the cyber-threats swells with the increase of personal devices with the rapid adoption of the BYOD trend. This research employed MSEM methods to develop a conceptual model based on Protection Motivation Theory by using data collected from 252 higher education students in a BYOD Australian university. Our findings confirmed and explored in details how intention to perform information security behaviours varied due to the change of context. Academics and practitioners could mitigate the security gap by focusing on the intention's differences discussed in our findings.*

**Keywords**

home user, information security behaviours, protection motivation theory, contextual differences

## INTRODUCTION

Information security behavioural research, despite its important roles in the overall defence, still falls short of contributions within the information security discipline (Crossler et al. 2013). On the other hand, the number of users' vulnerabilities is swelling every day. Indeed, Symantec (2013) reported that cyber-threats have switched their focus to social network activities and mobile devices in 2012. Such threats can be illustrated in the highest number of vulnerabilities found in mobile devices in 2012 (i.e. 415) compared to the previous year 2011 which was 315 (Symantec 2013). Further, a significant 58% increase of the mobile malware family plus the newly emerged mobile botnets attack continues to threaten both individuals and organisations' online safety (Symantec 2013). With the trending adoption of Bring Your Own Device (BYOD) policy that encourages uses of personal mobile devices (e.g. laptops, smartphones and tablets), such threats must not be overlooked.

Within the knowledge body of behavioural research in information security discipline, we found a large amount of studies focusing on employees' compliance and information security behaviours at workplace (e.g. Chan, Woon, & Kankanhalli, 2005; Herath & Rao, 2009; Seppo, Siponen, & Mahmood, 2007; Vance, Siponen, & Pahnila, 2012). In other words, the research landscapes were limited to only one context at a time. On the other hand, the domains of information security behaviours at home appear to be neglected thus suggest gaps in the field. Given the BYOD adoption that enables the mixing of personal devices uses across different contexts (e.g. from home to university as in this study's focus), we anticipate that information security behaviours may be influenced by such contextual change. In fact, uses of devices within public environments such as organisational intranets are usually protected by professional network security and guided by policy to ensure safe online practices. In contrast, private and less secure environments such as home offer even more freedom to many uses of devices, including those that invite cyber-threats. Similarly, Li and Siponen (2011) mentioned such differences as contextual factors and called for future research to focus on this matter. This study responds to Li & Siponen's call (2011) by investigating whether the intention to perform the same information security behaviours would be different between using the Internet on mobile devices at home and at public place. To achieve our research objectives, we developed an extended conceptual model based on Protection Motivation

Theory (PMT) from a sample of higher education (HE) students who are studying at a BYOD-enabled Australian university.

# THEORETICAL BACKGROUNDS

### Home User's Information Security Behaviours Against Malware

There are two distinctive streams of information security theories employed to understand how an individual defends against cyber-crimes. In particular, Liang & Xue (2009) argued that one can either avoid the cyber-threats or adopt safeguarding measures to prevent such threats from happening. In this study, we set focus on higher education (HE) students' intention to perform information security behaviours against malware. The rationale behind this focus is justified according to the following reasons.

First, the focus on Australian students' information security behaviours against malware addresses the critical issue displayed in the recent information security survey in 2008 (AusCERT 2008). Specifically, it reports a high amount of Australian's daily Internet activities including sending/receiving email (95%), surfing the web (88%), and downloading files (63%) (AusCERT 2008). In addition, while 79% of the participants of different ages and backgrounds claimed to have confidence in detecting malicious emails, 32% were found to click on links embedded in spam emails (AusCERT 2008). Referring back to the latest security report by Symantec (2013) which claimed 1 in 291 emails contains viruses, such statistics demonstrate that users are at high risk of being infected by malware from a simple, daily Internet activity. Second, prior studies such as the aforementioned ones have been investigating the contributing factors of employees' compliance. By including information security behaviours at home into our investigation, we differentiate our study with the others and join the few that study this domain. The HE students in our context are encouraged by BYOD policy to use their own mobile devices at university as at home, thus allows the comparisons of consistent conditions (i.e. same devices used for the same activities) in two different contexts.

### Contextual Difference and Information Security Behaviours

Originally, the study of Li & Siponen (2011) introduced four contexts including *work/non-work at home* and *at workplace* with their respective contextual factors. To stay consistent with Li & Siponen's (2011) contextual factors and our targeted sample of HE students, we need to align our study's contexts. By considering the Internet activities such as checking emails and browsing websites, we first bind the research landscape to *non-work* activities. Then, the *workplace context* suggested by Li & Siponen (2011) is replaced by *university context*. We argue that the university context in this study, while not being completely identical, shares common traits with the workplace's environment. Indeed, the BYOD policy allows the intranet's users to access the shared resources and applications from their personal devices. Further, there is policy dictated by the university to ensure that the users are conducting safe and productive practices on their own devices. However, there could be differences between workplace and university in how much the policy directs the users' purposes of using their devices. For example, office workers are more obliged to spend their time and granted resources for work purposes. In contrast, despite the students are encouraged to use their mobile devices to work on their assignments, they are not forbidden from playing games, accessing Facebook, and browsing unsafe websites. As a result, the university's policy appears to be more relaxed compared to the workplace's thus may invite more security risks. Next, the below discussions compare the two contexts in which the students could have different intention to perform adaptive behaviours.

*Using mobile devices at home*: There are two contextual factors when evaluating students' intention to perform non-work information security behaviours against malware at home: possible sharing computers and network security. Li and Siponen (2011) assert that sharing computers is one of the main differences between home and workplace contexts and this factor has impact on user's security behaviours. In our study, while the students can take ownership of their mobile devices (e.g. laptops or tablets) at university, there is a high chance that their family members may share the devices at home. Consequently, as users of different security knowledge and skills use the same devices for various purposes (e.g. study, play games and do shopping online), it becomes more difficult to manage the cyber-risks that such devices are exposed to. As a result, we could anticipate that the students' online safety is at greater risks when they use Internet at home in comparison to at university. In order to maintain online safety, the students may need to be more self-motivated and self-directed to perform information security behaviours at home.

*Using mobile devices at university*: Professional organisations such as universities invest in sophisticated information security infrastructure and thus the students are better protected against malware. The different network security clearly distinguishes the levels of information security at workplace and at home where the users are more prone to malware. As the adoption of the BYOD trend is increasing in today's organisations of

different sectors, universities also encourage students and staff to use their own devices in exchange for the benefits offered by this trend (Adhikari et al. 2006; Barkhuus 2005; Nykvist 2012). Therefore, organisations must continuously update information security policy that guides safe uses of their employees. In the educational context, the students can follow the instructions provided by the university's policy to minimise the risks of being infected by malware. In contrast, they are not bound to any strict guidance when using Internet at home and have more freedom to conduct riskier behaviours. Furthermore, being monitored under the policy also produces the effects of sanctions—the fear of being punished for violating the rules. In fact, this contextual factor was studied together with other constructs of Herath and Rao's (2009) PMT-based conceptual model, and it was found to have a small negative effect on compliance intention. Similarly, information security behaviours at home would not receive the influences of sanctions without the presences of policy and monitoring.

As such, we argue that there may be a difference in HE students' intention to perform information security behaviours against malware when they use their mobile devices at home and at university. Consequently, we hypothesised that the contextual difference could moderate the outcomes of the PMT's cognitive process (i.e. the causality of the cognitive process's constructs on the students' intention).

## HYPOTHESES DEVELOPMENT

Protection Motivation Theory (PMT) was originated from Rogers's study (1975) describing the antecedents of the human's cognitive process that motivate adaptive behaviours influenced by fear appeals. PMT was recently applied in behavioural information security studies to explain the users' intention to perform adaptive information security behaviours (e.g. Herath & Rao 2009; Johnston & Warkentin 2010; Pahnila, Siponen, & Mahmood 2007). Since we found no prior study applying PMT to investigate information security behaviours' distinctness caused by contextual differences, all possible relationships between the variables suggested by PMT will be examined for their potential distinctness between the two contexts. In particular, we are interested in answering the research question: *To what extent the impacts of the user's cognitive process on intention to perform information security behaviours have changed across the contexts*?

First we hypothesised the relationships between the PMT's components and HE students' intention to perform information security behaviours against malware. Through several modifications and developments, PMT comes up with a three-stage process starting from the source of information and other variables that influence a cognitive mediating process of evaluating the factors contributing to the appraisals of the threats and the coping solutions. While the source of information can vary, the cognitive process consists of six constructs in which three of each belongs to their respective appraisal. In particular, the threats appraisal captures the actor's perceptions of the threat's *vulnerability*, *severity* and advantages of committing a maladaptive behaviour (*rewards*). On the other hand, coping appraisal requires evaluation of the expected effectiveness of the adaptive behaviours (*response efficacy*), the expected trade-off of committing the desirable behaviours (*response cost*) and the actor's *self-efficacy*. After evaluating the threats and the recommended solutions in the second stage, the cognitive mediating process then influences the actor's protection motivation which finally guides the actual behaviours. The original model of PMT, which encapsulates the discussed hypotheses, is displayed in Figure 1.

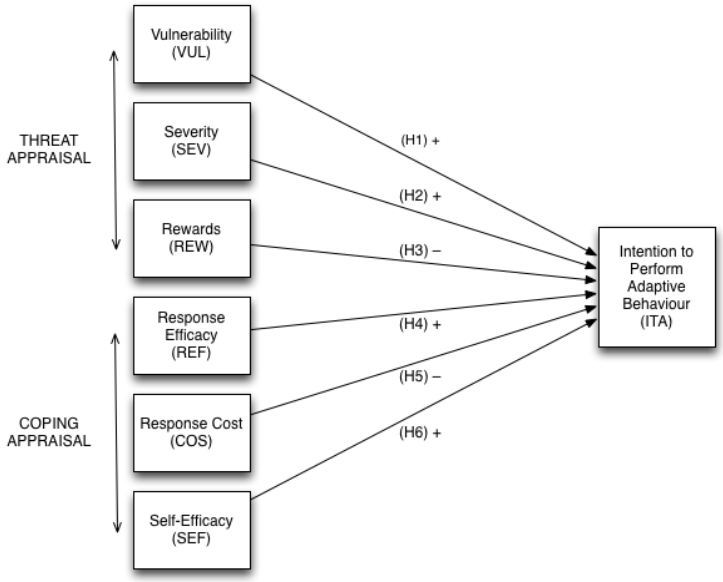


Figure 1: Conceptual model of PMT

*Threats Appraisals Cognitive Mediating Process*: The construct Vulnerability was originally introduced from PMT as the patient's perception of how probable it is to contract the disease (Rogers 1975). In the prior studies, this construct focuses on the employees' intention to comply with organisational security policy. *Vulnerability* is hypothesised to the employee's assessment of the organisation's exposure to cyber-threats (Herath and Rao 2009; Vance et al. 2012). These hypotheses suggest a focus on the actor's perception towards the community (i.e. the employee's organisation), and it may be confused with the actor's responsibility (as another potential construct) instead of perception about vulnerability. To avoid such confusion and align the construct with this study's context, we define the construct *Vulnerability* as the perception of how probably the students feel about themselves towards known and unknown cyber-threats which is consistent with the studies of Lee et al. (2008) and Mohamed and Ahmad (2012). As a result, we hypothesised that *perception about vulnerability motivates the students' intention to perform information security behaviours* (H1). Second, PMT defines *Severity* as the damage level of the diseases and the patients have more intention to perform recommended protection when their fear arises (Rogers 1975). Similar to *Vulnerability*, we identify two streams of defining this construct *Severity*: the first one measures the impacts of cyber-threats on the organisation (e.g. productivity, corporate data loss) and the other focuses on the damages suffered by individuals. Following our argument regarding *Vulnerability*'s impact on intention, we hypothesised that *perception about severity motivates the students' intention to perform information security behaviours* (H2). Third, PMT introduces the construct Advantages of Maladaptive Behaviour (Rogers 1975). This construct describes the actor's perception about the gains from conducting an undesirable action thus tempts the actor to commit such action. Likewise, Vance et al. (2012) conceptualises the same construct as *Rewards* which denotes the saved time and convenience from not conducting a security behaviour. In our context, we hypothesised that *perception about rewards discourages the students' intention to perform information security behaviours* (H3).

*Coping Appraisals Cognitive Mediating Process*: The Coping Appraisal process consists of the actor's perception towards his or her *self-efficacy* as well as the recommended solution, including its efficacy and cost (Rogers 1975). Following Vance et al. (2012) study which included hypothetical scenarios that capture participants' opinions about compliance, we introduced the best practices and recommendations about malware prevention to the students while they were answering the questionnaire. Among the questions involving such recommendations, there are those that ask the students to give their approvals to the information security behaviours' efficacy–how the recommended behaviours would successfully protect them against a malware contract. Accordingly, we hypothesized that *perception about response efficacy motivates the students' intention to perform information security behaviours* (Rogers 1975) (H4). Likewise, following the recommended behaviours would cost the students' time and cause inconvenience since they need to pay high attention to their daily activities' online safety, thus *perception about response cost discourages their intention to perform information security behaviours* (H5). Lastly, users could perform the recommended behaviours easily are indicated to be more willing to perform the solutions. Therefore, we hypothesised that *perception about self-efficacy motivates the students' intention to perform information security behaviours against malware* (H6).

## RESEARCH METHODOLOGY

Our research's nature follows the characteristics of positivism paradigm (Gartrell and Gartrell 1996). It aims to extend PMT to describe how contextual difference could influence user's cognitive process thus affects their intention to perform information security behaviours against malware across the contexts. To explain such phenomenon and evaluate the influences of the contextual difference, we decided to take a quantitative approach in this project. We designed and developed a 63-question survey (i.e. 7 questions about the participant's demographics and 2 sets of 28 six-point Likert scale questions about intention to perform information security behaviours in two contexts) to be sent to an anticipated sample size of 250 HE students. The six-point Likert scale was employed to enforce the participants not to choose "don't know" or "neutral" opinions. Our sample consists of HE students pursuing different degrees and program levels. We recruited them with a mixed-mode approach (i.e. offline and online modes) to reduce coverage error. As a result of a one-month survey using both online and in-person advertising channels, we retrieved back 282 responses in total with 30 invalid data resulting in a sample size of 252.

Our sample consists of a dominant group of students whose ages ranging from 18 to 21 years old (cumulate up to 63.1%) and completing Bachelor degrees (67.9%). Among these 252 students, 48.8% rated themselves to have "intermediate" information security skills and 31% considered to be "advanced" users. In addition, 142 of them selected iPhone as their BYOD–mobile devices of choice, followed by 104 Windows laptops and 90 Android smartphones. The most uses of mobile devices were to study (219 votes), entertainment–online music and games (206 votes) and communication–social networking and messaging (205 votes). Lastly, three equal durations of using the Internet per day were found to be 1–2 hours (20.2%), 3–4 (27%) and 5–6 (22.6%).

# DATA ANALYSIS

### Exploratory Factor Analysis (EFA)

The EFA process explores the patterns of the surveyed items (i.e. indicators) and determines the number of common factors (i.e. constructs) for the conceptual model (Brown 2006). In this research, we aimed to extract seven factors (referred to Figure 1) by using Principle Axis Factoring (PAF) and Direct Oblimin. As the use of Likert scales in the questionnaire returns multivariate non-normality data, our selection of PAF estimation method is justified since it is free of distributional assumptions (Brown 2006). On the other hand, we took advantage of the Direct Oblimin rotation technique which provides a "more realistic representation of how factors are interrelated" (Brown 2006 p. 32). We iterated the EFA process to eliminate indicators whose loadings did not exceed the suggested thresholds of 0.5, 0.45 and 0.35 (Lewis et al. 2005). As a result, indicators SEF4, REF4 and ITA4 were removed. Consequently, 25 indicators remained and formed seven common factors with KMO = 0.776 and Bartlett's test $p < 0.05$, meaning that factorability is acceptable (Hair et al. 2010).

### Multiple-Group Confirmatory Factor Analysis (MCFA)

In MCFA, we validated measurement models for each of the seven factors identified from the previous EFA process. This process included evaluating again convergent and discriminant validity among the factors and imputing them to generate the composited factor scores to be used in subsequent analyses by using AMOS. In convergent validity tests, seven measurement models were examined individually and re-specified to achieve desirable fit (i.e. $\chi^2$ $p$-value > 0.01; RMSEA < 0.06; SRMR < 0.07; CFI > 0.96) (Yu 2002) before being imputed. Besides evaluating construct reliability with Cronbach's α, coefficient H was also calculated to overcome the limitation caused by α's assumption on the measurement models to be essentially τ-equivalent (i.e. the same factor loading across indicators). Since our measurement models were congeneric (i.e. different factor loadings across indicators), such assumption was violated and the use of coefficient H as remedy for α's underestimation of the construct reliability was justified (Molla et al. 2011). In fact, coefficient H values should be larger than the α's for congeneric models. The overall results showed that all factors achieved excellent convergent validity (Table 1) while retaining all four indicators with good reliability (H, α > 0.07) for each measurement model.

Table 1: MCFA Convergent Validity Test

H stands for Home; U stands for University

| Factor | $\chi^2$ | df | $p$-value | RMSEA | SRMR | CFI | H (H) | α (H) | H (U) | α (U) |
|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

Discriminant validity tests were subsequently conducted to determine whether the factors are distinctive by comparing each average variance extract (AVE) against their squared correlations. As a result, factors that have AVE lower than their respective squared correlation are suggested to have discriminant validity issue. Our final results shown in Tables 2 and 3 indicate that all seven factors are distinctive in two contexts.

Table 2: 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 3: 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** |

**Multiple-group Structural Equation Modeling (MSEM)**

Finally, the validated factors were imputed to generate factor scores and put together to test the research model using MSEM. The original PMT-based model (Figure 1) displayed poor fit against the collected data: $\chi^2(30) = 364.382$; $p = 0.000$; RMSEA = 0.149; SRMR = 0.1692; CFI = 0.336. As a result, we respecified and extended the PMT-based conceptual model (Figure 2) which achieved excellent goodness-of-fit: $\chi^2(34) = 21.032$; $p = 0.960$; RMSEA = 0.000; SRMR = 0.0302; CFI = 1.000. MSEM was applied to evaluate the differences of cognitive process's outcomes in the two contexts (i.e. home and university) by comparing their respective effect sizes (β) using Cohen's interpretation (Cohen 1988). The hypotheses and the MSEM results conducted for two contexts are displayed in Table 4 and Figure 2 below. The value of Δβ is the absolute value of the difference of effect sizes between home and university contexts.

Table 4: MSEM Results

| | | Hypothesis | | | *p*-value | | Supported? | | β | | Δβ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Home | Uni | Home | Uni | Home | Uni | |
| | H1 | VUL | → | ITA | 0.064 | 0.021 | No | Yes | -0.037 | 0.074 | 0.111 |
| Original | H2 | SEV | → | ITA | 0.000 | 0.000 | Yes | Yes | 0.121 | 0.117 | 0.004 |
| PMT-based | H3 | REW | → | ITA | 0.021 | 0.021 | No | No | 0.060 | 0.065 | 0.005 |
| Hypotheses | H4 | REF | → | ITA | 0.000 | 0.000 | Yes | Yes | 0.234 | 0.196 | 0.038 |
| | H5 | COS | → | ITA | 0.000 | 0.000 | Yes | Yes | -0.187 | -0.176 | 0.011 |
| | H6 | SEF | → | ITA | 0.000 | 0.000 | Yes | Yes | 0.191 | 0.295 | 0.104 |
| | H7 | VUL | → | REF | 0.064 | 0.064 | No | No | -0.073 | -0.053 | 0.020 |
| | H8 | SEV | → | REF | 0.000 | 0.000 | Yes | Yes | 0.332 | 0.297 | 0.035 |
| | H9 | REF | → | SEF | 0.000 | 0.000 | Yes | Yes | 0.393 | 0.441 | 0.048 |
| Extended | H10 | REF | → | REW | 0.021 | 0.000 | Yes | Yes | 0.042 | 0.133 | 0.091 |
| PMT-based | H11 | REF | → | COS | 0.000 | 0.000 | Yes | Yes | -0.216 | -0.246 | 0.030 |
| Hypotheses | H12 | SEF | → | COS | 0.000 | 0.000 | Yes | Yes | -0.364 | -0.414 | 0.050 |
| | H13 | VUL | → | COS | 0.064 | 0.005 | No | Yes | -0.041 | -0.141 | 0.100 |
| | H14 | REW | → | COS | 0.001 | 0.001 | No | No | -0.112 | -0.128 | 0.016 |
| | H15 | SEV | → | COS | 0.902 | 0.064 | No | No | 0.007 | -0.017 | 0.024 |

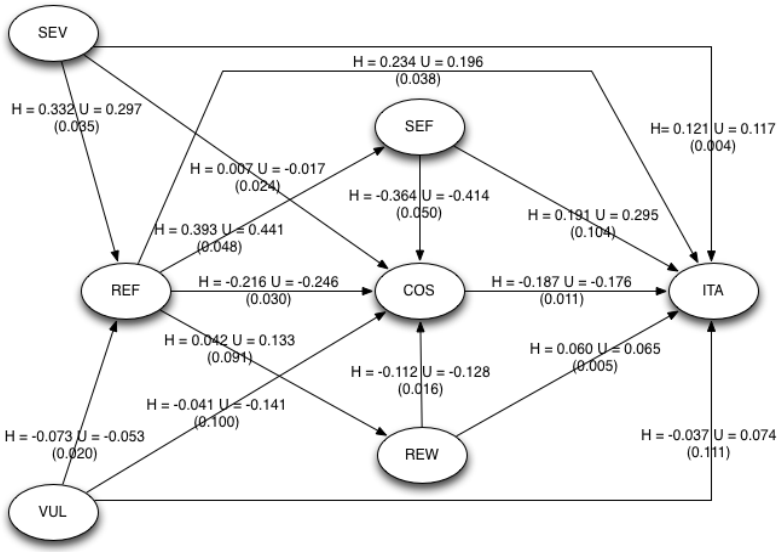


Figure 2: MSEM results (figures in brackets are Δβ)

# DISCUSSION

### Original PMT-based Hypotheses

In overall, our findings confirmed the different levels of impacts that the cognitive process's factors had on the students' intention to perform information security behaviours against malware in the two contexts. To begin with, we detected trivial differences in the causalities from perceived *severity* ($\Delta\beta_{ITA,SEV} = 0.004$), *response cost* ($\Delta\beta_{ITA,COS} = 0.011$), *rewards* ($\Delta\beta_{ITA,REW} = 0.005$) and *response efficiency* ($\Delta\beta_{ITA,REF} = 0.038$) to the students' *intention to perform* information security behaviours against malware across home and university contexts. First, an ignorable difference of perceived *severity*'s impact reflected the fact that the users might have overlooked the damages caused by malware on the public resources, hence evaluated the severity in both contexts solely based on their own devices' safety. If such reason held true, it could further suggest the potential involvement of the individual's responsibility over community's online safety in information security behavioural research.

Second, given the university's supporting defence mechanisms, the students' intention to perform still received no considerable change in the impact of the solutions' *cost* compared to performing them at home. This brought two controversial conjectures. It could simply reflect the fact that the students went through the same process to perform the same coping solutions, thus did not affect much the degree of costs in the two contexts. On the other hand, it could also suggest that the supporting defence either failed in reducing the inconvenience of performing the coping solutions or in helping the users to realise so. Therefore, education and training are essential to promote information security behaviours by demonstrating the corporate's capability and supports towards such practices.

Third, we found H3's result fail to support our initial hypothesis and contradict the original PMT as well as similar studies' findings (Mohamed and Ahmad 2012; Vance et al. 2012). Accordingly, the similar degree of trivial effects of *rewards* in both contexts motivated the students to perform the adaptive behaviours. As unusual as the result read, one possible conjecture was that the students had no choices but still performed the information security behaviours despite realising their inconveniences. Indeed, such outcome could reflect the unique characteristics in this sample of HE students whose security knowledge and perceptions about vulnerability and severity might be different from the employees that were researched in other studies. Given the finding's inconsistent nature with PMT and other studies, practitioners should only consider this finding in non-work contexts and especially in the higher education sector.

Similar to the above discussion on the solutions' *cost*, H4 suggested that the students perceived the *efficacy* of recommended information security behaviours to have similar effects on their intention in both contexts. This finding did not support our anticipation that the students would be more motivated by the recommended behaviours' effectiveness at home since they may have no choice but rely solely on their own actions, unlike at university where they would receive more supports from the corporate network security. While it is good that the students can realise and be motivated by the *response efficacy* in both contexts, practitioners are advised to promote better additional supports from the organisation's defence that could help to boost such effectiveness– e.g. firewall can filter and block more malicious websites and emails than the user's self-awareness.

On the other hand, small differences were found in the impacts of students' perceptions about *vulnerability* ($\Delta\beta_{ITA,VUL} = 0.111$) and *self-efficacy* ($\Delta\beta_{ITA,SEF} = 0.104$) on their *intention to perform* information security behaviours. Specifically, the factor *self-efficacy*, which measures the beliefs in the ability and power to accomplish a task (Luszczynska and Schwarzer 2005), was more influential on the students' intention at university than at home. Given such result and definition, we could posit that different *self-efficacy*'s beliefs about the same coping solutions were created depending on the contexts in such a way that the students intend to perform the behaviours more at university. This finding raised the need for future research to investigate whether contextual *self-efficacy* would exist in the domain of information security behavioural research.

More important, we found that the impact of perceived *vulnerability* on the students' *intention to perform* the recommended behaviours only existed in university context ($p = 0.021$). This could be interpreted that only when using mobile devices at university (or public places) the students would be more motivated to protect themselves against malware because they feel vulnerable to the cyber-threats. Practitioners should not overlook this slight difference and underestimate the weaker impact of *vulnerability* on *intention to perform* at home as it could be the sign of a greater security gap in the future if no preventive actions are taken. On the other hand, another possible reason was that the construct *vulnerability* had different meanings as perceived by the students depending on the contexts, and we may have to measure it differently.

**Extended PMT-based Hypotheses**

Using MSEM allowed us to discover nine relationships between independent variables across the two contexts that are not explained in the original PMT, although we only discuss the seven statistically significant ones (i.e. H8–H14). First of all, the trivial differences in the new relationships include the gaps between the positive influences of *severity* on *response efficacy* ($\Delta\beta_{REF,SEV} = 0.035$), *response efficacy* on *self-efficacy* ($\Delta\beta_{SEF,REF} = 0.048$) and *rewards* respectively ($\Delta\beta_{REW,REF} = 0.091$). Specifically, we did not find a considerable change of impact by perceived severity on the coping solutions' effectiveness across the two contexts. This finding was reasonable since the same sets of coping solutions were introduced to the students in both contexts. Besides the confirmed gap of impact, our finding suggested a medium driving effect of severity on the solutions' effectiveness. Practitioners could educate the users more about the severity of being infected by malware thus encourages their adoption of the coping solutions.

The next trivial difference was in the causalities from *response efficacy* to *self-efficacy*. Accordingly, there was an ignorable change in how the students measured the solutions' effectiveness by their ease of use. Similar to the above explanation about the same set of adaptive behaviours were introduced, we also found medium effect sizes in this pair of causalities across the contexts. Indeed, this emphasised the importance of usability which contributes to the users' perception about the solutions' effectiveness. On the other hand, the factor *rewards* was found in another unusual causality in which it received positive contribution from response efficacy. One possible explanation was that the students perceived our study's suggested information security behaviours to be effective but not convenient enough to overcome the rewards of not performing them in both contexts.

Other trivial differences were about the students' perception about *response cost* received stronger negative impacts from *response efficacy* ($\Delta\beta_{COS,REF} = 0.030$) and *self-efficacy* ($\Delta\beta_{COS,SEF} = 0.050$) in university context. The findings reflected the situation in which the students did not find much changes in how the solutions' benefits (i.e. efficiency and usability) could overcome their inconveniences, regardless of the contextual differences. Again, such outcomes were foreseeable when we used the same set of solutions in our questionnaire. More important, we found *self-efficacy* and *response efficacy* produced medium-sized impacts that reduce the costs experienced by the users in both contexts. As consistent with the results of the PMT original hypotheses, these results reflected the current stability across the contexts. Therefore, we would advise organisations and practitioners to maintain such small gaps while improving the overall information security equally by considering the causalities from these extended hypotheses.

Lastly, we found the same outcome occurred to the relationship between *vulnerability* and *response cost* ($\Delta\beta_{COS,VUL} = 0.100$) in which it was only significant in university context. In other words, the perception of being vulnerable to malware at home failed to reduce the users' perception about the coping solutions' costs. This further supported our previous conjecture about the possibility of two different meanings of the *vulnerability* construct were created depending on the contexts. Therefore, we strongly encouraged future research to investigate more about the user's perceptions about their *vulnerability* to cyber-threats. Since perceived *vulnerability* may associate with fear, our suggestion was consistent with the call for future attention on the facets of fear by Crossler et al. (2013) and we believed such topic will yield interesting findings.

## LIMITATIONS AND CONCLUSION

Given the rigorous methodology and data analyses discussed above, our research contains some limitations. First, the sample contained only HE students. Even though the sample consisted of students from different programs with varied knowledge and skills in information security, it may not represent the whole population of Internet users. As a result, there could be potential changes in the intention to perform information security behaviours between different pairs of contexts and our findings may only be applicable in the educational sector. Second, our research only tested two out of four contexts as suggested in the study of Li and Siponen (2011). In fact, our results displaying slight differences in the intention to perform information security behaviours might be due to the lack of seriousness and commitment in the uses of mobile devices for *non-work* purposes. Therefore, future studies may investigate further the differences of information security behaviours between other contexts such as *work at home* and *work at workplace*.

The findings have answered our research question and Li and Siponen's (2011) call for research investigating the impacts of contextual difference on the user's intention to perform information security behaviours. To the best of our knowledge, our research was among the first few studies that investigated intention to perform information security behaviours in more than one context, especially the uses of mobile devices in home environment that is commonly less secure than workplace. Given the increase of BYOD adoption that mixes private uses into public contexts and the accompanied cyber-threats that target personal devices, our findings were necessary. Specifically, our extended PMT-based model confirmed the small differences in how the users'

cognitive process forms their intention to perform safe online behaviours against malware between the two contexts. The findings also discussed the possible reasons behind such differences that reflect how the users perceive when using their devices in a BYOD environment. While only small differences were detected in this study's contexts between home and university, we could anticipate more interesting changes in office workers' intention to perform information security behaviours (e.g. compliance) when it involves work's seriousness and commitment. By taking this study as an initiative, we encourage future research to proceed on investigating such differences in workplace BYOD environment. Before that, academics and practitioners are recommended to raise awareness about such differences and prepare to mitigate the information security gaps caused by the emerging practices of BYOD policy.

Moreover, our findings also suggested that there may exist different meanings of the constructs *self-efficacy* and *vulnerability* according to the contexts in which the users use their mobile devices. Such findings revealed the theoretical gaps in behavioural research field and suggested directions for future investigations. Understanding more about these constructs would definitely be useful for better management of information security, particularly for those that adopt BYOD policy. For instance, information security programs could be designed to enforce and motivate how the users perceive their *self-efficacy* accurately according to the contexts thus raises their confidence in handling cyber-threats in different situations. On the other hand, knowledge about their perceptions of *vulnerability* in each context would help practitioners to gain better focus on why the users fear cyber-threats. To illustrate, we found in our contexts that the students were motivated to perform adaptive behaviours by the perception of being vulnerable only at university. This sole finding posed many questions to us: which factors have formed their *vulnerability* at university but not at home? Why home context lacks those factors, hence resulted in the lack of motivation from *vulnerability*? Does *vulnerability* actually exist in home context, or it exists with a different definition (e.g. an overall vulnerability of the whole family but not just the individual perceiving it)? By answering these questions, information security measures could be tailored better to either mitigate the particular *vulnerability* in different contexts, or exploit them as means to motivate information security behaviours more effectively. As our study has confirmed such phenomenon and its similar ones (i.e. the constructs *rewards* and *self-efficacy*) in our findings, we leave the explorations to future studies.

## REFERENCES

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

AusCERT. (2008), *Home Users Computer Security Survey 2008*, Brisbane, Australia. Retrieved from http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf

Barkhuus, L. (2005), "'Bring Your Own Laptop Unless You Want to Follow the Lecture': Alternative Communication in the Classroom," *Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work. ACM, 2005.*, pp. 140–143.

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

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security in the workplace: linking information security climate to compliant behavior," *Journal of information privacy and security*, no. PriceWaterHouseCoopers, pp. 18–41.

Cohen, J. (1988), *Statistical power analysis for the behavioral sciences*, Routledge.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research," *Computers & Security*, Elsevier Ltd, vol. 32, pp. 90–101.

Gartrell, C.D. and Gartrell, J.W. (1996), "Positivism in Sociological Practice: 1967-1990," *Canadian Review of Sociology*, vol. 33 no. 2, pp. 143–158.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2010), *Multivariate Data Analysis*, Upper Saddle River, NJ: Prentice Hall, 7th ed.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18 no. 2, pp. 106–125.

Johnston, A.C.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study," *MIS Quarterly*, vol. 34 no. 3, p. 549.

Lee, D., Larose, R. and Rifon, N. (2008), "Keeping our network safe: a model of online protection behaviour," *Behaviour & Information Technology*, vol. 27 no. 5, pp. 445–454.

Lewis, B.R., Templeton, G.F. and Byrd, T.A. (2005), "A methodology for construct development in MIS research," *European Journal of Information Systems*, vol. 14 no. 4, pp. 388–400.

Li, Y. and Siponen, M. (2011), "A CALL FOR RESEARCH ON HOME USERS' INFORMATION SECURITY BEHAVIOUR," *15th Pacific Asia Conference on Information Systems (PACIS)*.

Liang, H. and Xue, Y. (2009), "AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE," *MIS Quarterly*, vol. 33 no. 1, pp. 71–90.

Luszczynska, A. and Schwarzer, R. (2005), "Social cognitive theory," *Predicting health behaviour, 2*, vol. 2, pp. 127–169.

Mohamed, N. and Ahmad, I.H. (2012), "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior*, Elsevier Ltd, vol. 28 no. 6, pp. 2366–2375.

Molla, A., Cooper, V. and Pittayachawan, S. (2011), "The Green IT Readiness (G-readiness) of Organisations: An Exploratory Analysis of a Construct and Instrument," *Communications of the Association for Information Systems*, vol. 29 no. 1.

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

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, no. 91, pp. 93–114.

Seppo, P., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance," *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on. IEEE*, p. 156b–156b.

Symantec. (2013), *INTERNET SECURITY THREAT REPORT 2013*, Moutain View, USA, Vol. 18. Retrievedfrom http://www.symantec.com/security_response/publications/threatreport.jsp

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49 no. 3–4, pp. 190–198.

Yu, C.-Y. (2002), *Evaluating Cutoff Criteria of Model Fit Indices for Latent Variable Models with Binary and Continuous Outcomes*, University of California, Los Angeles.

## COPYRIGHT