Computers in Human Behavior 87 (2018) 87–97

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full Length Article

Costly but effective: Comparing the factors that influence employee anti-malware behaviours

John M. Blythe*, Lynne Coventry

PaCT Lab, Department of Psychology, Northumbria University, Newcastle Upon Tyne, NE1 8ST, UK

ABSTRACT

A cross sectional survey examined an extended version of Protection Motivation Theory (PMT) to identify factors that influence employees' intentions to perform three anti-malware behaviours. 526 employees completed an online survey that measured an employees' threat (severity and susceptibility) and coping (self-efficacy, response efficacy and response costs) appraisal. The survey also extended PMT to include additional factors of experience, psychological ownership, organisational citizenship and security responsibility. Factors were found to have differing effects on employees' intentions to engage in anti-malware behaviours indicating the importance of targeted behavioural analyses. From PMT, coping appraisal was more predictive of security behaviours than threat appraisal. Specifically, across all behaviours, response costs were identified as a key factor that may be a barrier to behaviour whereas response efficacy was a key facilitator. Moreover, additional factors to extend PMT contributed unique variance to predicting each anti-malware behaviour. The study highlights the importance of identifying key factors prior to intervention development and demonstrates the benefit of expanding on behavioural theories to account for factors that may be important for the cybersecurity context.

1. Introduction

Users are continually exposed to a variety of online threats (such as malware and phishing emails) that put their information and privacy in danger. The risks to organisations are even greater as they face more advanced and persistent threats (Symantec, 2017), as well as, the insider threat. The insider threat is employees who introduce risks to information security due to non-compliance with their organisation's information security policy (CPNI, 2017). Understanding the insider threat and employees' security behaviour is therefore key to successful information security (Coventry, Briggs, Blythe, & Tran, 2014).

In 2017, around 50% of UK organisations experienced at least one security breach in the last year (DCMS, 2017). These breaches can have damaging effects as 46% of organisation's reputations are impacted as a result of a security breach (Forbes, 2014). For example, in October 2015, TalkTalk experienced a major breach resulting in the leak of 156,000 customer's personal details. As a result, TalkTalk lost an estimated £60 million in revenue and 95,000 of their customers went to their competitors (Telegraph, 2016). Employees often account for a proportion of these security breaches, figures from the Ponemon Institute (2015) indicate that 25% of breaches were due to employee's insecure behaviours, 29% were due to system glitches and the remaining 46% were due to malicious attacks. Recently, DCMS (2017) found that 72% of breaches were due to staff receiving and acting on phishing emails. These figures demonstrate the importance of understanding and reducing the threat that arises from insecure employee behaviour.

Malware threats continue to be one of the frequently experienced cyberattacks (Information-age.com, 2016). Despite companies' best efforts, attacks remain relatively stable with malware variants rising significantly from 50.1 million to 96.1 million from September 2016 to October 2016 (Symantec, 2016). Indeed, 12 million new malware variants are being discovered monthly with more malware being discovered between 2014 and 2016 than in the previous 28 years combined (Symantec, 2016). Malware can financial and reputational effects on organisations and even disrupt the running of major public services. In May 2017, the WannaCry ransomware targeted machines running Microsoft Windows, encrypting data and demanding a "ransom" in bitcoin payment. This cyberattack was experienced worldwide affecting more than 230,000 computers in over 150 countries within one day (Seccomglobal, 2017). The attack impacted on the running of major public services including the National Health Service in the United Kingdom.

Malware can infect organisations through many routes such as hidden on USB sticks and distributed through phishing emails. USB sticks can store hidden malware which can easily spread across

* Corresponding author.
E-mail addresses: john.blythe@hotmail.co.uk, j.blythe@ucl.ac.uk (J.M. Blythe), lynne.coventry@northumbria.ac.uk (L. Coventry).

https://doi.org/10.1016/j.chb.2018.05.023
Received 25 August 2017; Accepted 20 May 2018
Available online 21 May 2018

computers as the user shares or plugs their USB device into other machines. For phishing emails, users can infect their machines through downloading infected attachments or visiting infected websites via links within an email. The tactics used by attackers are variable, often changing the way malware is distributed by email. For example, in October 2014 only 7% of phishing emails contained malicious links, this rose to 41% in November 2014 and continued to rise through December (Symantec, 2014). The success of malware relies on targeting the vulnerabilities of computer systems and software. For example, drive-by downloads exploit vulnerabilities in web browsers or plugins that allow malware to be installed on users' machines. Software such as Java, Flash and Adobe Acrobat have been used as platforms for attackers to install malware on users' machines and these need to be kept up to date (Microsoft, 2015). Security software and operating system updates are important to ensure vulnerabilities are quickly removed. Attackers take advantage of zero-day exploits in which attackers exploit vulnerabilities in software that are unknown to the software provider (Sans, 2015) and through users delayed updates. Users can prevent the success of these malware threats by using anti-malware software to scan USB sticks to prevent malware (GetSafeOnline, 2018), avoiding links in suspicious emails (Ion, Reeder, & Consolvo, 2015) and installing software updates when prompted (Cyberaware, 2018; Ion et al., 2015). However, studies have indicated only 17% of users who plug in unknown USB sticks have scanned them for malware (CompTIA, 2015), 25% of users click on suspicious links rising to 45% when the email is personalized to the user (Benenson, 2016) and 38% of users update immediately (Ion et al., 2015), with users postponing longer for certain programs (Nappa, Johnson, Bilge, Caballero, & Dumitraş, 2015).

Preventing malware threats involves technical, procedural and behavioural approaches. The most common behavioural approach is the use of information security polices and awareness campaigns (Coventry et al., 2014). These polices dictate employees' responsibilities for cybersecurity, however they are often poorly designed as the responsibilities placed on users are not aligned with their productivity goals (Beautement, Sasse, & Wonham, 2009). This leads users to bypass procedures or adopt less secure but more productive security behaviours (Kirlappos, Parkin, & Sasse, 2015). Furthermore, awareness campaigns do not often target the key reasons why people do not behave securely and are largely unsuccessful (Bada, 2014). There is debate regarding how much responsibility should be placed on employees for cybersecurity and a successful organisational approach to reducing malware would be a technical and procedural approach that is underpinned with behavioural insights. One route to this is to understand the reasons why employees do not engage in security behaviours and to then design interventions that span both the user and organisational level.

The current study focuses on behavioural approaches to reducing malware as it is a prevalent threat faced by organisations and indices indicate that employees do not always engage in behaviours that help to prevent this threat. We focus on the following behaviours: use of anti-malware software to scan USB sticks ('anti-malware software'), avoiding links in suspicious emails ('email security') and installing software updates when prompted ('software updates'). We chose important behaviours covering these different avenues (anti-malware software, email security and software updates) in which malware can infect organisations. The behaviours were chosen as they are important behaviours to prevent malware and require different levels of input from the user so may provide potential variation in the reasons why employees do not engage in anti-malware behaviours. This paper explores factors that affect employee's intentions to engage in these three behaviours. To achieve this, participants completed an online survey assessing their intentions to perform the three anti-malware behaviours and measures assessing Protection Motivation Theory (PMT; Rogers, 1975) constructs. The study sought to expand a theoretical model based upon PMT by also including understudied factors identified in previous research. The study seeks to address the following research questions:

1. What are the key factors that influence employee's intentions to engage in anti-malware behaviours?
2. How does the influence of these key factors differ by anti-malware behaviour?
3. Does an extended-Protection Motivation Theory model explain more variance in intention to engage in anti-malware behaviours than the original Protection Motivation Theory model?

2. Theoretical model development

To understand why employees do not perform anti-malware behaviours, it is important to consider the driving forces behind behaviours using theories from behavioural science. In doing so we can understand the processes that underpin security behaviours. By identifying the causes of secure and insecure behaviour, interventions can be designed to promote secure behaviour based on the strength of the relationships between the theoretical constructs and the security behaviour of interest. Presently, cybersecurity behavioural interventions are not designed using theory and often rely on the "educate and train the user" approach (Coventry et al., 2014) without addressing the key factors that influence behaviour. Interventions that are based on theory and target the key factors are more likely to be effective in changing behaviour (Michie, van Stralen, & West, 2011).

There are many theories that can be used to understand security behaviour and existing studies have utilised constructs from behavioural theories such as Protection Motivation Theory (e.g. Ifinedo, 2011), Theory of planned behaviour (e.g. Bulgurcu, Cavusoglu, & Benbasat, 2010), Health Belief Model (Davinson & Sillence, 2014), or may study the whole theory in isolation (e.g. Dang-Pham & Pittayachawan, 2015) in an attempt to explain as much variance as possible in the outcome variable (e.g. intention to perform behaviours). We seek to extend a theory of behaviour change (Protection Motivation Theory; PMT) based upon a sub-set of factors identified in existing qualitative research (Blythe, Coventry, & Little, 2015).

Protection motivation theory (PMT) focuses on how people appraise a threat and their ability to cope with that threat. The theory posits that behaviour results from a decision-making process in which people undergo a threat and coping appraisal. *Threat appraisal* consists of their assessment of the consequences of a threat ('perceived severity') and the extent to which they believe they will be affected by a threat ('perceived susceptibility'). *Coping appraisal* considers how they will prevent the threat by evaluating their ability to enact recommended courses of action successfully ('self-efficacy'), expectations of the efficacy of the action in reducing the threat ('response efficacy') and costs associated with taking the course of action ('response costs'). This threat and coping appraisal is part of PMT which was developed by Rogers (1975) to explore the effects of an individuals' risk perception on behaviour. Combined, the threat appraisal and the coping appraisal influence individual's intention to protect themselves (Boer & Seydel, 1996). A number of studies have adopted PMT to explore cybersecurity behaviours (e.g. Chenoweth, Minch, & Gattiker, 2009; Shillair et al., 2015; Siponen, Mahmood, & Pahnila, 2014).

Whilst work has begun to explore the driving forces underlying security behaviours in a workplace setting (e.g. Herath & Rao, 2009; Ifinedo, 2014), these define security behaviour as "*intention to comply with the IS policy*" which reduces compliance into a single behaviour. This presents a number of problems as it: (1) relies on employees awareness of the content of the policy when answering questions, (2) does not recognise the multitude of different behaviours encapsulated

in a policy, (3) assumes that what motivates one behaviour (such as use of strong passwords) will motivate a completely different behaviour (such as downloading software updates) and (4) does not allow comparisons as organisations differ in the content of their policies (Blythe et al., 2015). There is a lack of focus on specific behaviours in the workplace and those which do focus on single behaviours tend to focus on private use of technology rather than workplace use (e.g. Crossler, 2010; Gurung, Luo, & Liao, 2009; Lee, Larose, & Rifon, 2008; Zhang & McDowell, 2009).

Using an extended-PMT model (see Fig. 1), the current study aims to identify key factors related to employees' intentions to engage in three types of anti-malware behaviours: an anti-malware software behaviour (using anti-malware software to scan USB sticks for malware), an email security behaviour (not clicking on links in suspicious emails) and a software update behaviour (installing software updates when prompted). In the following subsections, we detail the specific components and hypotheses of PMT and the additional factors to extend the PMT model.

2.1. Threat appraisal

Threat appraisal consists of perceived severity and perceived susceptibility. Perceived severity is "*the negative consequences an individual associates with an event*" (e.g. a security threat). For malware threats, this may be consequences towards employees' productivity, the functioning of their devices and their organisation's reputation. Research has shown that employees with higher perceptions of severity are more likely to comply with their organisation's information security policy (Siponen et al., 2014; Vance, Siponen, & Pahnila, 2012). However, for home users, the role of severity is not so clear cut. Research has shown severity to predict anti-spyware adoption (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2009) but not for a backing up data (Crossler, 2010) and password protection (Zhang and McDowell (2009).

Perceived susceptibility is the "*extent to which individuals feel they are at risk of a threat*". Research has also supported a positive relationship between perceived susceptibility and information security policy compliance (Ifinedo, 2011; Siponen et al., 2014). However, recently, Crossler, Long, Loraas, and Trinkle (2014) found that susceptibility did not influence intention or actual compliance to Bring Your Own Device policies. Interestingly, susceptibility did not influence use of anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009) in home settings. These findings suggest that suscepbility's role in security behaviours may differ by behaviour and context.

A limitation of the existing research in the workplace is that they do not focus on severity or susceptibility of specific security threats but rather uses items that refer to the broad term "security threats". Only a few studies focus on the specific security threats in their items such as viruses (D. Lee et al., 2008; Ng, Kankanhalli, & Xu, 2009), wireless hacking (Woon, Tan, & Low, 2005) and spyware (Gurung et al., 2009; Liang & Xue, 2010) however they have not been explored in an organisational context. Recently, Blythe et al. (2015) found that employees perceived cybersecurity threats to be more likely than physical threats, indicating that employees feel more susceptible to cybersecurity threats. However, understanding the influence of susceptibility on malware threats in the workplace requires further investigation.

The current study seeks to explore a specific cybersecurity threat - malware in an organisational context. Based on PMT and existing research, we therefore test the relationships between employees' threat appraisal (perceived severity and perceived suscepbility) and their intention to (i) use anti-malware software to scan USB sticks for malware, (ii) not click on links in suspicious emails and (iii) install software updates when prompted.

2.2. Coping appraisal

Coping appraisal consists of self-efficacy, response efficacy and response costs. Self-efficacy can be defined as "*an individual's beliefs about their competence to cope with a task and exercise influence over the events that affect their lives*" (Bandura, 1977). In a security context, employees who have high security-related capabilities are presumed to be more likely to follow security practices as they are more effective in learning how to follow them and being able to perform the appropriate behaviour.

Self-efficacy has consistently been shown to relate to information security policy compliance (Bulgurcu et al., 2010; Crossler et al., 2014; Ifinedo, 2011, 2014; Sommestad, Karlzén, & Hallberg, 2015; Vance et al., 2012) and a range of specific behaviours such as being cautious with email attachments (Ng et al., 2009) and complying with password guidelines (Mwagwabi, McGill, & Dixon, 2014).

The second component of coping appraisal is response efficacy and is "*belief in the benefits of the behaviour*" (Rogers, 1983). In the case of security, this is the belief that performing security behaviours is an effective way to reduce security breaches. Research has supported a positive relationship with intention to adopt anti-spyware software (Johnston & Warkentin, 2010; Liang & Xue, 2010), backing up data (Crossler, 2010) anti-spyware usage (Gurung et al., 2009; Liang & Xue, 2010), compliance with password guidelines (Mwagwabi et al., 2014), adopting password protective behaviours in students (L. Zhang & McDowell, 2009) and enabling security measures on home wireless networks (Woon et al., 2005). However, the influence of response efficacy on IS policy compliance intention has been inconsistent (Crossler & Bélanger, 2014; Ifinedo, 2011; Vance et al., 2012; Wall, Palvia, & Lowry, 2013; J. Zhang, Reithel, & Li, 2009).

The final component of response appraisal is response costs and refers to "*beliefs about how costly performing the recommended security behaviour will be*". These costs may include money, time, and effort expended in behaving securely or other negative consequences, which result from performing the security behaviour. Research findings are inconclusive on the role of response costs. Herath & Rao (2009) found support for a negative relationship between response costs and information security policy compliance intention whereas Ifinedo (2011) and Crossler et al. (2014) did not find support for response costs. Mixed findings have also been reported between response costs and anti-spyware adoption (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2010) and other research has found no support for response costs in employees' email security behaviour (Ng et al., 2009)) and backing up behaviour (Crossler, 2010). However, a wealth of qualitative research supports the costly nature of security behaviour and its impact on employee productiviy (Albrechtsen, 2007; Beautement et al., 2009; Inglesant & Sasse, 2010).

Based upon PMT and existing research, we therefore test the relationships between employees' coping appraisal (self-efficacy, response efficacy, and reponses costs) and their intention to (i) use anti-malware software to scan USB sticks for malware, (ii) not click on links in suspicious emails and (iii) install software updates when prompted.

2.3. Prior experiences

Prior experiences can be both negative and positive and can potentially influence security behaviour in different ways. Negative experiences such as a malware infection or having your personal account (such as Facebook) hacked can result in many negative emotional states for the user such as frustration, annoyance, and embarrassment. They can also have more severe consequences such as the potential for financial loss and identity theft. Employees may experience threats personally at home or within their work environment. For example, when people experience a privacy invasion, they are likely to perceive greater

vulnerability and severity of the risk (Petronio, 2012). Experiencing such situations may heighten a user's threat and coping appraisal of that threat. Subsequently, this may lead to adoption of security behaviours. Within PMT, experience is one source of intrapersonal information which influences individuals' threat and coping appraisal and their intention to act and can be defined as "*feedback from personal experiences associated with the targeted maladaptive and adaptive responses*" (Floyd, Prentice-Dunn, & Rogers, 2000), p. 409). Protection motivation theory posits that the relationship between prior experience and intention is mediated through threat and coping appraisal (Maddux & Rogers, 1983). However, the role of experience is often understudied in existing research using protection motivation theory (Floyd et al., 2000; Milne, Sheeran, & Orbell, 2000). A recent study by Chen, Beaudoin, and Hong (2016) explored prior experiences of stolen information (such as banking details, unauthorized access to email) on privacy protective behaviour and found that it was mediated by the users' awareness of their online information disclosure habits. Other studies have shown that threat and coping appraisals mediated experience on protective behaviours (Demuth, Morss, Lazo, & Trumbo, 2016). This supports an indirect role of prior experience on protective behaviours.

Other studies have suggested a more direct influence on protective behaviour. Lee et al. (2008) found a significant direct relationship between prior virus experience and intentions to engage in anti-virus protective behaviours in students. Individuals who had a computer virus were more motivated to protect themselves. Experience of security threats, therefore, appears to influence current behaviour directly and indirectly. We therefore first test a direct relationship between employees' prior experience (personal or work-related) and their intention to (i) use anti-malware software to scan USB sticks for malware, (ii) not click on links in suspicious emails and (iii) install software updates when prompted. We then test an indirect relationship by assessing whether employees' threat appraisal (susceptibility & severity) and coping appraisal (response efficacy, self-efficacy and response costs) mediates this relationship.

2.4. Extending protection motivation theory with additional factors

We identified factors from a previous qualitative study based on PMT (Blythe et al., 2015) that were acknowledged as key factors that may influence employee security behaviour but have not been explored quantitatively. Firstly, Blythe et al. found that employees evaluate the sensitivity of the information that they work with and this linked to their motivation to engage in security behaviour. Other research has shown that employee perceptions of sensitivity interacted with their perceptions of security (Adams & Sasse, 1999) as commercially sensitive information was considered less sensitive than information about living individuals. Employees' appraisal of the sensitivity of their work data may therefore influence their intentions to engage in security behaviours to protect it.

Secondly, Blythe et al. found that employees were empowered to take responsibility for some behaviours but not others. They found that employees relied on security experts in their company for anti-malware protection but would take personal responsibility for passwords. Individuals with higher perceived security responsibility may therefore intend to engage in anti-malware behaviours.

Furthermore, information security research presently gives little attention to the antecedents of behaviour in organisations. Behaviour becomes more complex under the constraints of different environments (Michie et al., 2011) so greater consideration is needed on potential organisational factors that may influence employees' behaviour. Two unexplored factors that may be important for security behaviour in the workplace are organisational citizenship behaviour and psychological ownership.

Psychological ownership is defined as a state in which individuals experience a possessive connection with targets they feel are "theirs" (Pierce, Kostova, & Dirks, 2003). These feelings of ownership can occur regardless of whether or not the individual legally owns the object and includes objects used by employees that are the property of their organisation (Pierce et al., 2003). These targets can be physical items such as work computers and non-physical targets such as ideas and creative works. Higher levels of psychological ownership towards a target can lead to enhanced protective strategies (Dipboye, 1977; Korman, 1970). In the context of work, if employees perceive that they own the data they create and/or their work computer they may engage in more security behaviours to protect them. Previously, psychological ownership of one's computer was significantly related to intention to perform security-related behaviour in home users (Anderson & Agarwal, 2010). Feelings of ownership towards devices and data in the workplace may increase the likelihood of protective strategies. Further research is required to explore its potential role in employee security behaviour.

Organisational citizenship behaviours (OCB) are positive organisational behaviours defined as '*discretionary contributions that go beyond the strict job description and that do not lay claim to contractual recompense from the formal reward system*' (Organ, 1988). They go beyond an individual's job performance and relate to behaviours that contribute to the optimal functioning of the organisation These individuals "go above and beyond" the minimum requirements of their job role and as such, organisations benefit from increased productivity, efficiency and customer satisfaction when employees engage in OCB (N. P. Podsakoff, Whiting, Podsakoff, & Blume, 2009). The importance of OCB has been demonstrated in occupational psychology literature and has been found to have many benefits for organisations such as higher unit sales (P. M. Podsakoff & MacKenzie, 1997) and increased job performance (MacKenzie, Podsakoff, & Ahearne, 1998). The role of OCB in the security context has remained unexplored. However, it would be expected that individuals who engage in discretionary behaviours may engage in more security-related actions. Further research on the role of OCB in information security is required.

In light of the factors identified in a qualitative PMT study by Blythe et al. (workplace information sensitivity appraisal and security responsibility) and factors that have been previously underexplored in cybersecurity (psychological ownership of data and technology, and organisational citizenship behaviour), we seek to extend the original PMT model and explore the added variance that may be explained by assessing the relationships between these additional factors and intention to (i) use anti-malware software to scan USB sticks for malware, (ii) not click on links in suspicious emails and (iii) install software updates when prompted.

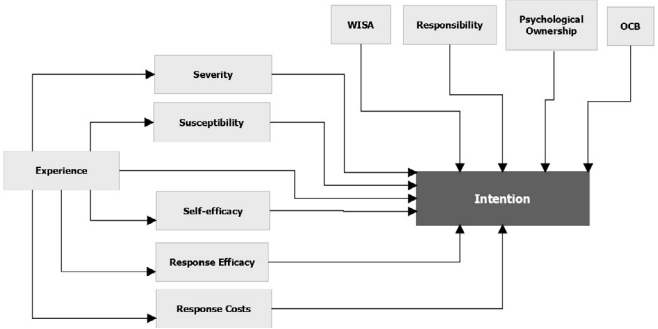

Fig. 1. Hypothesized Extended Protection Motivation Theory in the context of security.

3. Method

3.1. Design

A cross sectional correlational design was adopted to understand the relationship between the predictors (threat appraisal, coping appraisal and additional factors) and outcome variables (intention to engage in *using anti-malware software to scan USB sticks for malware, not clicking on links in suspicious emails and installing software updates when prompted*).

3.2. Participants

An opportunity sample of 526 (Age, M = *35.52*, SD = *12.22*) individuals were recruited online. Participants were eligible to take part if they were (i) aged 18 or above, (ii) in full time or part employment and (iii) used an email and computer as part of their daily work tasks. Opportunity sampling was used to recruit participants using a variety of platforms based on recruitment recommendations from Branley, Covey, and Hardey (2014) which included dedicated participation sites (e.g. callforparticipants.com), social media (e.g. Facebook, Twitter, LinkedIn), mailing lists, websites and forums. Snowballing sampling technique was used to recruit participants in order to maximise recruitment, this involved encouraging participants to share the study with their acquaintances by retweeting the study link on Twitter or sharing the recruitment advertisement on Facebook. See Table 1 for a full overview of participant demographics.

Table 1
Participant demographics.

Variable	N = 401
Gender	
Male	38%
Female	61%
Prefer not to say	1%
Read information security policy	
Yes	55%
Unsure	13%
Never read policy	22%
Organisation did not have policy	10%
If Yes,	
Read the policy within the last month	10%
Last 1–6 months	29%
6–12 months ago	18%
More than 12 months	23%
Not sure	20%
Enterprise size	
Microenterprise (less than 10 staff)	8%
Small enterprise (less than 50 staff)	9%
Medium-sized enterprise (less than 250 staff)	10%
Large organisation (more than 250 staff)	73%
Device used most for work task	
Desktop PC	71%
Laptop	26%
Smartphone	1%
Tablet	2%
Device owner	
Company-owned device	84%
Personally-owned device	16%
Operating system	
Microsoft Windows	83%
Mac OS X	13%
Linux	2%
iOS	1%
Android	1%

To control for organisational differences in information security policies, participants were only eligible to complete the "Anti-malware software" section of the survey dependent upon their organisation's information security policy i.e. if participants answered "Yes" to whether their organisation allowed them to use USB sticks and they had access to anti-malware software. This resulted in different sample sizes for each behaviour. 422 completed the software update section, 324 completed the anti-malware software section and 428 completed the email security section. All recruited participants were currently in full time or part time employment with an average organisational tenure of 6.19 years (SD = *7.31*) and job tenure of 3.81 years (SD = *5.17*). 36% of participants had managerial responsibilities. Power analysis indicated that this sample was sufficient to detect a medium-to-large effect size ($f = 0.25$) with a power of 80% at a standard Type I error rate ($\alpha = 0.05$).

3.3. Measures

Unless otherwise stated all items were measured on a five point Likert scale that ranged from (1) strongly disagree to (5) strongly agree.

3.3.1. Threat appraisal

Perceived susceptibility was measured with four items. Two items were taken from Johnston and Warkentin (2010) in which the security threat was changed from spyware to malware. Two items were also based on Milne, Orbell, and Sheeran (2002) and were re-worded to reflect the area of security e.g. "*My chances of developing CHD in the future are*" was changed to "*My chances of infecting my work device with malware in the future are high*". The scale had an internal reliability of $\alpha = 0.72$.

Perceived severity was measured with 13 items. Three items were based on Johnston and Warkentin (2010) such as "*If my work device were infected by malware, it would be severe*". The remaining 10 items were self-developed and were based on the findings from Blythe et al. . The inclusion of these items was to target the four areas of potential consequences (technological, personal, 3rd party and organisational) as identified by Blythe et al. An example item is "*If my work device were infected by malware, I could be severely disciplined".* The total scale had an internal reliability of $\alpha = 0.88$.

3.3.2. Response appraisal

The following constructs were measured for each of the three security behaviours. All the items were the same except the beginning of the sentence; here it is represented as < security behaviour > .

Response efficacy was measured with 13 items. Three items were based on Witte, Cmaeron, McKeon, and Berkowitz (1996) response efficacy template such as " < *security behaviour* > *works in preventing malware*". Additional items were included to assess ratings of response efficacy for avoiding the negative consequences associated with the security threat as previous studies mainly focus on threat reduction in response efficacy measures. In line with perceived severity, these targeted the four areas of threat consequences. An example item is " < *security behaviour* > *works in protecting the reputation of my organisation".* The internal reliability was $\alpha = 0.95$ for anti-malware software, $\alpha = 0.95$ for email security and $\alpha = 0.95$ for software updates.

Self-efficacy was measured with four items based on Milne et al. (2002) such as "*I feel confident in my ability to* < *security behaviour* > ". The internal reliability was $\alpha = 0.85$ for Anti-malware software, $\alpha = 0.84$ for email security and $\alpha = 0.84$ for software updates.

Response costs were measured with two items based on Gurung et al. (2009) and expanded with additional items that measured the associated costs of the specific security behaviour. Anti-malware software had an additional seven items such as "*Using the anti-malware software on my device to scan for malware would slow my device down*". The security behaviour installing updates had an additional six items such as "*Installing operating system updates on my work device could lead to a less reliable or 'buggy' software version being installed*". Finally, not clicking on links in suspicious emails had four additional items such as "*not clicking on URL links in suspicious emails would affect my productivity at work*". The internal reliability was $\alpha = 0.84$ for anti-malware software, $\alpha = 0.89$ for email security and $\alpha = 0.87$ for software updates.

3.3.3. Additional factors

Prior experience was self-developed and consisted of 12 items. Six items measured employees' direct personal experience of the consequences of security breaches and the other six items measured experience of these breaches in the workplace. An example of an item "*My personal account (e.g. email, social media) has been used by someone without my permission*". The scale had an internal reliability of α = 0.83.

Security Responsibility was a self-developed seven item scale in which participants scored themselves on a 7-point visual analogue scale from "my company's responsibility" to "my responsibility". An example item is *"to install anti-malware software on devices I use for work*". The scale had an internal reliability of α = 0.81.

Workplace Information Sensitivity Appraisal was measured using the WISA scale consisting of 16 items (Blythe, 2015). Participants rate the sensitivity of information that they work with. The full-scale had an internal reliability of α = 0.78. The internal reliabilities for the sub-scales were α = 0.82, consequences α = 0.79, worth α = 0.85, low proximity interest α = 0.75 and for high proximity interest α = 0.94.

Psychological ownership was measured using four items based on the scale from Anderson and Agarwal (2010) in which the target was changed to reflect the work computer and work data. Two items measured the sub-scale of psychological ownership of work data (e.g. *I feel a high degree of personal ownership for the data stored on the computer I use at work*). A further two items measured the sub-scale of psychological ownership of the work computer (e.g. *I sense that the computer I use at work is MINE*). The full-scale had an internal reliability of α = .87. The sub-scale for data ownership had an internal reliability of α = 0.80 and for device ownership α = .87.

Organisational citizenship behaviour was measured using the OCB-O questionnaire developed by Lee and Allen (2002). The scale consists of eight items (e.g. I *defend the organisation when other employees criticise it*). The scale had an internal reliability of α = 0.85.

3.3.4. Intention

Intention was measured with three items based on Johnston and Warkentin (2010) such as "*I intend to < security behaviour > in the next 2 weeks*". < time element > was specific to situation. The internal reliability for intention for anti-malware software (α = 0.92), for email security (α = 0.88) and for software updates (α = 0.93).

3.4. Procedure

Before commencement of this study, full ethical approval was received from the Faculty of Health and Life Sciences Ethics Committee at Northumbria University. All participants accessed the study on the Qualtrics survey platform and recruited through social media, mailing lists, online forums, posters and through emails distributed by the university. Each behaviour was presented in a separate section and questions were randomised. Each section presented instructions to participants, explaining key terms and images to help participants with answering the survey items. On completion, participants were given the option to enter a prize draw to win an iPad, thanked for their participation and were provided with debrief information.

4. Results

4.1. Data analysis strategy

We adopted a multi-stage process to test the hypotheses. Firstly, we identified relationships between the variables. We then employed hierarchical regressions to identify which factors predict behavioural intention.

4.2. Preliminary analyses

First, the data was screened for multi-collinearity, missing data and outliers. Variance inflation factors were checked for multi-collinearity issues, all factors ranged from 1.13 to 2.04 for all behaviours and therefore were below the conservative cut-off of 3 (Bowerman & O'Connell, 1990; Petter, Straub, & Rai, 2007) indicating that multi-collinearity was not present. The data file was split into three representing each behaviour and expectation–maximization estimation was performed on the data to retain as many participants as possible. This was only permitted where items had less than 10% missing data. Inspection of the data indicated that there were no outliers.

See for Table 2 for descriptive statistics.

Table 2
Descriptive statistics for variables under investigation.

Variable	Mean	SD
Workplace Information Sensitivity Appraisal (Privacy)	4.03	0.78
Workplace Information Sensitivity Appraisal (Consequences)	2.10	0.81
Workplace Information Sensitivity Appraisal (Worth)	4.40	0.68
Workplace Information Sensitivity Appraisal (Low proximity)	3.25	0.87
Workplace Information Sensitivity Appraisal (High proximity)	1.72	0.93
Perceived susceptibility	2.21	0.73
Perceived severity	3.49	.66
Organisational Citizenship Behaviour (OCB)	3.58	0.68
Personal security experience	1.89	0.25
Work security experience	2.05	0.38
Psychological ownership – Data	3.74	1.12
Psychological ownership – Technology	2.05	0.38
Responsibility	2.94	0.83
Self-efficacy (Anti-malware software)	3.69	0.89
Response efficacy (Anti-malware software)	3.72	0.63
Response costs (Anti-malware software)	2.62	0.67
Self-efficacy (Email security)	4.52	0.72
Response efficacy (Email security)	4.08	0.64
Response costs (Email security)	1.55	0.81
Self-efficacy (Software update)	3.73	1.03
Response costs (Software update)	2.73	0.84
Response efficacy (Software update)	3.37	0.69
Anti-malware software intention	3.54	0.99
Software update intention	3.32	1.1
Email security intention	4.67	0.65

4.3. Exploring the theoretical models

4.3.1. Anti-malware software (scanning USB sticks with anti-malware software): hierarchical regression

Hierarchical regression was employed to explore the additional factors to the initial PMT framework. The first step included all predictors from PMT using the enter method. These were the following predictors: susceptibility, self-efficacy, response efficacy, response costs and severity. The second step used the stepwise method to add each additional factor (responsibility, workplace information sensitivity appraisal, experience, OCB, psychological ownership) to the initial PMT model.

The findings from the regression analyses (see Table 3) shows that model 1 is able to account for 37% of the variance in employees' intentions to scan USB sticks with anti-malware software (R^2 = .37, F (5,318) = 36.57, $p < .001$) with self-efficacy as the strongest significant predictor (β = .447, $t(318)$ = 9.109, $p < .001$), followed by response costs (β = -0.187, $t(318)$ = -3.934, $p < .001$), and response efficacy (β = .182, $t(318)$ = 3.762, $p < .001$). The addition of responsibility contributed to an increase in R^2 of 2% in model 2 (R^2 = .39, F (1,317) = 12.974, $p < .001$) in which responsibility was a significant predictor (β = .166, t (317) = 3.602, $p < .001$). In the final model, the addition of workplace information sensitvity apprasial (consequences) was a significant predictor (β = .118, t (316) = 2.543, $p < .01$) and contributed to an increase in R^2 of 1% (R^2 = .40, F (1,316) = 6.467, $p < .05$). The addition of responsibility and workplace information sensitivity appraisal (consequences) predicts unique variance in the behaviour.

Table 3
Coefficients for Model 1, Model 2 and Model 3 following hierarchical regression for scanning USB sticks with anti-malware software.

	B	SE B	β
Model 1			
Constant	1.429	.464	
Perceived susceptibility	.092	.063	.067
Perceived severity	-.079	.073	-.050
Self-efficacy	.500	.055	.447***
Response efficacy	.285	.076	.182***
Response costs	-.277	.071	-.187***
Model 2			
Constant	.874	.481	
Perceived susceptibility	.087	.062	.063
Perceived severity	-.039	.072	-.025
Self-efficacy	.452	.056	.404***
Response efficacy	.278	.074	.177***
Response costs	-.275	.069	-.185***
Responsibility	.207	.057	.166***
Model 3			
Constant	.770	.479	
Perceived susceptibility	.069	.062	.050
Perceived severity	-.059	.072	-.038
Self-efficacy	.466	.055	.417***
Response efficacy	.279	.074	.178***
Response costs	-.318	.071	-.214***
Responsibility	.191	.057	.154**
WISA (Consequences)	.153	.060	.118*

Note. $R^2 = 0.37$ for model 1. $\Delta R^2 = 0.02$ for model 2. $\Delta R^2 = 0.01$ for model 3. *p < .05 **p < .01 ***p < .001.

Overall, the final model consisting of the following significant predictors (in order of contribution to regression): self-efficacy, response costs, response efficacy, responsibility and workplace information sensitivity appraisal (consequences) explain 40% of the variance in employees' intentions to scan USB sticks with anti-malware software.

4.3.2. Email security (not clicking on links in suspicious emails): hierarchical regression

The findings from the regression analyses suggested that the final model accounted for 47% of the variance in employees' intentions to not click on suspicious links within emails. Self-efficacy was found to contribute the most, followed by response costs, security breach experience at work, susceptibility and response efficacy.

The findings from the regression analyses, as shown in Table 4, shows that model 1 is able to account for 46% of the variance in employees' intentions to not click on links in suspicious emails ($R^2 = .46, F (5,422) = 70.890, p < .001$) with self-efficacy as the strongest significant predictor ($\beta = .489, t(422) = 10.302, p < .001$), followed by response costs ($\beta = -0.174, t(422) = -3.779, p < .001$) and response efficacy ($\beta = .089, t(422) = 2.198, p < .05$).

Table 4
Coefficients for Model 1 and Model 2 following hierarchical regression for not clicking on links in suspicious emails.

	B	SE B	β
Model 1			
Constant	2.773	.273	
Perceived susceptibility	-.063	.034	-.070
Perceived severity	.002	.037	.002
Self-efficacy	.419	.041	.489***
Response efficacy	.091	.042	.089*
Response costs	-.140	.037	-.174***
Model 2			
Constant	2.828	.271	
Perceived susceptibility	-.086	.034	-.097*
Perceived severity	.000	.036	.000
Self-efficacy	.417	.040	.487***
Response efficacy	.087	.041	.085*
Response costs	-.147	.037	-.183***
Experience at work	.085	.028	.111**

Note. $R^2 = 0.46$ for model 1. $\Delta R^2 = 0.01$ for model 2. *p < .05 **p < .01 ***p < .001.

In the final model, the addition of security breach experience at work was a significant predictor ($\beta = .111, t (421) = 3.002, p < .01$), alongside contributing susceptibility to the prediction ($\beta = -0.097, t (421) = -2.533, p < .01$) led to an increase in R^2 of 1% ($R^2 = .47, F (1,421) = 9.012, p < .01$).

Overall, the final model consisting of the following significant predictors (in order of contribution to regression); self-efficacy, response costs, security breach experience at work and perceived susceptibility explain 47% of the variance in intentions to not click on links in suspicious emails.

4.3.3. Software updates (installing software updates when prompted): hierarchical regression

The findings from the regression analyses, as shown in Table 5, shows that model 1 is able to account for 26% of the variance in employees' intentions to install software updates when prompted ($R^2 = .26, F(5,416) = 28.667, p < .001$) with response efficacy as the strongest significant predictor ($\beta = .306, t(416) = 6.798, p < .001$), followed by response costs ($\beta = -0.248, t(416) = -5.120, p < .001$), and perceived susceptibility ($\beta = .152, t(416) = 3.539, p < .001$). In model 2, the addition of responsibility was a significant predictor ($\beta = .148, t (415) = 3.403, p < .01$) and contributed to an increase in R^2 of 2% ($R^2 = .28, F (1,415) = 11.578, p < .001$) predicting unique variance in the behaviour. In the final model, the addition of psychological ownership of data was a significant predictor ($\beta = .086, t (414) = 1.980, p < .05$) and contributed to an increase in R^2 of 0.7% ($R^2 = .28, F (1,414) = 3.921, p < .05$).

Overall, the final model consisting of the following significant predictors (in order of contribution to regression); response efficacy, response costs, perceived susceptibility, responsibility and psychological ownership of data explains 28% of the variance in employees' intentions to install software updates when prompted.

Table 5
Coefficients for Model 1 and Model 2 following hierarchical regression for installing software updates when prompted.

	B	SE B	β
Model 1			
Constant	1.313	.471	
Perceived susceptibility	.231	.065	.152***
Perceived severity	.066	.073	.039
Self-efficacy	.133	.050	.125**
Response efficacy	.490	.072	.306***
Response costs	-.324	.063	-.248***
Model 2			
Constant	.845	.485	
Perceived susceptibility	.214	.065	.140***
Perceived severity	.090	.073	.054
Self-efficacy	.096	.050	.090
Response efficacy	.479	.071	.299***
Response costs	-.321	.063	-.245***
Responsibility	.200	.059	.148**
Model 3			
Constant	.624	.496	
Perceived susceptibility	.210	.065	.138**
Perceived severity	.091	.072	.055
Self-efficacy	.094	.050	.088
Response efficacy	.478	.071	.299***
Response costs	-.313	.062	-.239***
Responsibility	.169	.061	.125**
Psychological ownership of data	.083	.042	.086*

Note. $R^2 = 0.26$ for model 1. $\Delta R^2 = 0.02$ for model 2. $\Delta R^2 = 0.007$ for model 3. *p < .05 **p < .01 ***p < .001.

4.3.3.1. Exploring the effects of threat and coping appraisal mediating the relationship between prior experience and intentions. We hypothesized that threat *(susceptibility & severity)* and coping appraisal *(response efficacy, self-efficacy and response costs)* will mediate the relationship between prior experience (personal or work-related) and intention.

We only tested mediation for email security because it was the only analysis to have a direct effect between work-related prior experience and intention to not click on links in suspicious emails meeting conditions outlined by Baron and Kenny (1986).

The conditions for full mediation analysis were, however, not met (Baron & Kenny, 1986) because work-related prior experience was not related to the hypothesized mediators: coping appraisal ((response efficacy *($\beta = -0.192$, $t(396) = -2.313$, $p < .054$)*, self-efficacy *($\beta = -0.174$, $t(396) = -1.714$, $p < .087$)*, response costs *($\beta = -0.112$, $t(396) = -1.009$, $p < .313$)* and threat appraisal (susceptibility *($\beta = -0.001$, $t(396) = -0.008$, $p < .994$)*, severity *($\beta = -0.135$, $t(396) = -1.545$, $p < .123$)*. The findings, therefore, suggest that the effect of work-related prior experience on intention to not click on links in suspicious emails is not mediated by threat and coping appraisal.

5. Discussion

5.1. The key factors that influence intentions to perform anti-malware behaviours

5.1.1. Coping appraisal

Response costs were identified as a key factor for all behaviours with a negative relationship indicating a significant barrier. The influence of response costs was strongest for the anti-malware software behaviour, followed by software updates and finally, the email security behaviour. Employees who perceive that anti-malware behaviours have high costs (such as loss of productivity, effort and time) are less likely to intend to perform the behaviours. The relationship between response costs and security behaviour is consistent with studies exploring the relationship with anti-spyware software in consumers (Chenoweth et al., 2009; Liang & Xue, 2010), and adds to the body of knowledge in this underexplored area and the notion of security impacting on employee productivity (e.g. Beautement et al., 2009). Reducing responses costs through re-designing information security policies and procedures is therefore essential to reduce costs on users (Beautement et al., 2009). This can achieved by aligning security with user goals (Beautement, Becker, Parkin, Krol, & Sasse, 2016).

Response efficacy was shown to be a key influencer of intention to perform all anti-malware security behaviours. Response efficacy has been regarded as one of the worst predictors of compliance (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014) as the existing research has been inconsistent either supporting a positive relationship (Ifinedo, 2011; Wall et al., 2013; L. Zhang & McDowell, 2009), a negative relationship (Vance et al., 2012) or finding no relationship (Siponen, Pahnila, & Mahmood, 2010). The current study shows that response efficacy is important for security behaviour when focusing on specific behaviours and security threats. This is in line with PMT which posits that behaviour is enhanced by beliefs that it is effective in reducing threats. Employees perceive that all three behaviours are important in reducing malware threats. Of the three behaviours, the email security behaviour was perceived to be the most effective in preventing malware, followed by the anti-malware software behaviour and finally, the software update behaviour. However, the relationship was strongest for the anti-malware software security behaviour.

Self-efficacy was the strongest predictor for the anti-malware software and the email security behaviour but did not influence the software update behaviour. The lack of support for the software update behaviour indicates that employees' beliefs in their capabilities is not important for installing software updates when prompted. This highlights that perceptions of capability are not important for all security behaviours, installing software updates may be perceived as an easy behaviour to perform as this may involve responding to a dialog box and, therefore, other factors may be better able to explain the lack of engagement. On the other hand, the anti-malware software and email security behaviours require a level of skill. The first requires the user to know how to access and run the anti-malware software and the email security behaviour requires the users to have the ability to detect suspicious links. The current study supports the existing research on the role of self-efficacy in using anti-spyware software (Gurung et al., 2009; Y.; Lee & Kozar, 2008; Liang & Xue, 2010) and those exploring email security behaviour in relation to malware threats (Ng et al., 2009). There is little research looking at software update behaviour. However, the current study suggests that for potentially passive behaviours that require less input from the user, self-efficacy may not be important for motivating employees to undertake them but rather factors such as a negative attitude towards updating (Fagan, Khan, & Buck, 2015) and physical opportunity to install updates (Michie et al., 2011) may be more important.

5.1.2. Threat appraisal

The current study does not support previous research showing a significant relationship between perceived severity and compliance intention (Chenoweth et al., 2009; Gurung et al., 2009; Siponen et al., 2014; Vance et al., 2012) and intentions to adopt anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009; Liang & Xue, 2009). However, the current study does support D. Lee et al. (2008) and Ng et al. (2009) who found that severity did not affect anti-virus protection behaviours and being cautious with emails with attachments respectively. The lack of support could be due to a number of factors. Firstly, there are few studies exploring specific security threats in the workplace as the majority that do focus on specific types (e.g. malware) have been a home context. This study, alongside Ng et al. (2009), are the only studies to explore malware threats in an employment sample and both did not find a direct relationship to intention. Within the workplace setting, employees may perceive the severity of malware threats to be less severe. Meta-analytic research exploring the efficacy of PMT in other domains has found that severity and intention have the weakest association amongst all of the PMT relationships (Milne et al., 2000). The current study suggests that employees' perceptions of the severity of malware are not important for driving anti-malware behaviour.

The second aspect of threat appraisal, susceptibility, was also found to differing relationships with security behaviour. The current study found that it was a significant predictor of software update intention supporting research by D. Lee et al. (2008) who found that susceptibility was a significant predictor of installing operating system updates. The current study found that susceptibility did not predict the anti-malware software behaviour which is supportive of other research that has found no role for susceptibility in consumers use of anti-spyware software (Chenoweth et al., 2009; Gurung et al., 2009).

The relationship between susceptibility and the email security behaviour was in the opposite direction to what is posited by PMT (Rogers, 1975) with lower levels of susceptibility indicative of greater intention to perform the behaviour. This is unexpected, as according to PMT, individuals with greater perceived susceptibility to malware would be more likely to adopt behaviours to prevent it. The current study suggests, however, that for email security behaviour, susceptibility may be a barrier. This may be because suspicious links are associated with information disclosure or phishing scams (Getsafeonline.org, 2015) rather than the distribution of malware. There is also a lack of research in exploring malware and email behaviour, however, Ng et al. (2009) found that susceptibility of malware attachments influenced cautious email behaviour. There may be differences in relation to link behaviour in emails as employees may not perceive email links to be associated with malware threats. Instead, they may associate malware in emails with attachments rather than links. The majority of research exploring organisational security

behaviour has been supportive of the link between susceptibility and behaviour, however, a number of these studies do not focus on specific security threats (Herath & Rao, 2009; Ifinedo, 2011; Siponen et al., 2014). The current study explored a specific security threat: malware and found malware susceptibility to have differing effects on behaviours highlighting users' inability to connect behaviours to specific threats.

5.1.3. Additional factors

Experience of security issues at work were also found to significantly influence the email security behaviour. After self-efficacy, it was the strongest predictor of the behaviour indicating that experience of the negative aspects of security/computer related issues in the workplace influences email-related security behaviour. Experience is considered within PMT to be mediated by threat and coping appraisal. However, the current study found that it was not mediated by the threat and coping appraisal. The role of experience is relatively understudied in existing research focusing on PMT in security research. However, the findings do support Blythe et al. (2015) which found that experiencing the negative consequences of security threats influenced security behaviour. The current study suggests that experience may only have a direct role on some security behaviours. For email security, experiencing the negative consequences of security issues may promote awareness and greater detection surrounding email phishing.

The current study found that the workplace information sensitivity appraisal factors did not influence the software update or email security behaviour. There was partial support for the anti-malware software behaviour in which the consequences component of workplace information sensitivity appraisal significantly related to intention, suggesting that employees who have a greater perception that the disclosure of the data they work with has consequences (such as compromising and discreditable) intend to scan USB sticks with anti-malware software to protect the information. Employees working with information that has the potential for serious consequences if disclosed may, therefore, have greater motivation to protect it in relation to USB stick usage and anti-malware software. This was the first study to specifically explore the role of workplace information sensitivity appraisal for a specific security threat and sub-set of behaviours.

The current study found that responsibility was a strong predictor of anti-malware software and software update security. Individuals with higher perceptions of personal responsibility for security had greater motivation to undertake anti-malware actions. This supports the findings from Blythe et al. that employees may diffuse responsibility onto third parties for certain behaviours. Interestingly, the findings from Blythe et al. suggested that employees were more likely to perceive behaviours such as virus prevention as the responsibility of their organisation. However the current study suggests that employees with a sense of responsibility for security are likely to undertake anti-malware behaviours pertaining to use of anti-malware software and installing software updates. Empowering users with a sense of responsibility is, therefore, important to promote uptake of behaviours. The lack of support for the email security behaviour may be due to the level of involvement. The anti-malware software and software update behaviours are required to be performed less frequently than the email security behaviour. Employees regularly use email as part of their job so may actively carry out the behaviour daily. Due to the repeated occurrences, the behaviour may become more habitual and therefore, not require a conscious deliberation on responsibility.

Psychological ownership was only related to the software update behaviour. The findings indicated that feelings of ownership of data influenced intentions to update the software. The affective components of ownership are apparent when others lay claim to objects/target for which an individual has a sense of ownership (Pierce et al., 2003). Employees may feel that by not updating their work devices, that the data may be in jeopardy and therefore feel empowered to protect the data. No existing studies have explored the influence of psychological ownership on security behaviour in the workplace. The study does support Anderson and Agarwal (2010) who found ownership perceptions influenced home users' intentions to perform security behaviours.

The current study also found no support for a relationship between organisational citizenship behaviour and intentions. This does not support Blythe et al. who found that employees who engage in actions that aided the organisation in business continuity and recovery may have better security behaviour. The lack of support could be due to the measure that was used in the current study. The scale adopted was a well-validated scale and looks at OCB broadly within the organisation by exploring citizenship behaviours that contribute to the optimal functioning of the organisation. A specific measure looking at security citizenship behaviours may have shown a direct relationship. Future research could, therefore, develop and validate a measure of security citizenship behaviour to allow a more detailed exploration of the relationship.

5.2. Extending protection motivation theory

As the interest in behavioural insights around cybersecurity has grown so has the use of existing behaviour change models, which were originally developed for health behaviour but are now applied and refined for the cybersecurity context. The original PMT paper was developed by Rogers (1975) to understand how people appraise and respond to health threats. Whilst PMT has been used in existing cybersecurity research (e.g. Chenoweth et al., 2009; Liang & Xue, 2010), this has been limited due to poor conceptualisations and measurement of security threats and security behaviours (see Blythe et al., 2015). We show that by extending the PMT model with additional factors based on existing cybersecurity research and focusing on specific security threats and behaviours we were able to contribute unique variance to the model.

The current study found that by extending the PMT model, it could explain 40% of the variance in employees' intentions to scan USB sticks for malware, 28% of the variance in employees' intentions to install software updates and 47% of the variance in employees' email security behaviour. The variance explained for the anti-malware software behaviour and email security behaviour is line with other research using PMT, Chenoweth et al. (2009) explained 43% of the variance in consumers intentions to use anti-spyware software, whereas Liang and Xue (2010) explained 56% of users' intentions to use anti-spyware software. D. Lee et al. (2008) using PMT in combination with other theories explained 45% of the variance in a composite measure of anti-virus behaviours. Ng et al. (2009) used the Health Belief Model and explained 61% of the variance in being cautious with email attachments. The current study is line with those using PMT to explain users' behaviour; however it does mean 50–60% of the variance for these two behaviours is explained by factors not considered in the study. Future research would benefit from refining and testing behaviour change theories applied to cybersecurity behaviours.

5.3. Practical implications

The findings from this study have a number of practical implications for organisations seeking to improve the anti-malware behaviour of their employees. Firstly, as responses costs were identified as a key barrier to behaviour, where possible organisations should seek to reduce the time and productivity burden associated with anti-malware behaviours. This can be achieved by aligning security with user goals and work tasks (Beautement et al., 2016). For example, the UK government have started to publish guidance to re-design security policies that reduce time and productivity burden on employees (National Cyber Security Centre, 2017). Secondly, a common behaviour change technique used in interventions in organisations is to raise employees' fear of consequences (i.e. perceived severity) by scaring them about the consequences of not behaving securely (e.g. loss of company data,

identity theft etc.) (Coventry et al., 2014; Van Steen, 2017). However, the findings from this study indicate that perceptions of severity are not a key factor that influences anti-malware behaviour so this technique would not lead to behaviour change. Instead, organisations should choose behaviour change techniques that influence the key factors that impact on behaviours (Michie et al., 2013). For example, for increasing engagement in the anti-malware software and email security behaviours, companies could focus on enhancing self-efficacy through 'action planning', 'providing instruction' and 'reinforcing effort towards behaviour' as these techniques have been shown to effectively increase self-efficacy (Williams & French, 2011).

5.4. Limitations

Attempts were made to reduce common method bias, however as security behaviours can be considered to be a form of job performance, social desirability bias (P. M. Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) may have inflated participants intentions to engage in the behaviours. Furthermore, the study relied on self-report measures and actual performance measures would have been more beneficial. Future research would benefit from utilizing multi-method approaches to measuring security performance such as supervisor ratings (Harris & Schaubroeck, 1988) or objective logs from employees computers (Workman, Bommer, & Straub, 2008).

6. Conclusions

Protection motivation theory is a useful lens to identity the facilitators and barriers to anti-malware behaviours. Factors were found to have differing effects on employees' intentions to engage in anti-malware behaviours. Specifically, the study found that self-efficacy, response efficacy and security responsibility were significant predictors of employees' intentions to scan USB sticks with anti-malware software. For employees' intentions to not click on links in suspicious emails, self-efficacy, security breach experience at work and perceived susceptibility were significant predictors. Finally, for intentions to install software updates when prompted, response efficacy, response costs, perceived susceptibility, responsibility and psychological ownership of data were significant predictors. Response costs were also found to be a significant negative predictor of all three behaviours indicating a barrier to anti-malware behaviours. Extending PMT with additional factors was found to have different predictive contributions depending on behaviour. Future work will focus on using this information to target the factors in behaviour change interventions.

Acknowledgements

This work was supported by an internal PhD funded studentship from Northumbria University. We would also like to thank Dr. Julia Yesberg for her assistance with revisions of the paper.

References

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46. https://doi.org/10.1145/322796.322806.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004.

Anderson, C., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly, 34*(3), 613–643.

Bada, M. (2014). *Cyber Security Awareness Campaigns Why do they fail to change behaviour?* Global Cyber Security Capacity Centre Draft Working Paper, (July).

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. https://doi.org/10.1037//0033-295X.84.2.191.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173–1182. https://doi.org/10.1037//0022-3514.51.6.1173.

Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, M. A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. *Proceedings of the symposium on usable privacy and security (SOUPS)* (pp. 1–18). .

Beautement, A., Sasse, M., & Wonham, M. (2009). The compliance budget: Managing security behaviour in organisations. *In Proceedings of the 2008 workshop on New security paradigms* (pp. 47–58). . https://doi.org/10.1145/1595676.1595684.

Benenson, Z. (2016). *How to make people click on dangerous links despite their security awareness*USA: Blackhat. 2016. Retrieved from https://www.blackhat.com/docs/us-16/materials/us-16-Benenson-Exploiting-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous-Link-Despite-Their-Security-Awareness.pdf.

Blythe, J. M. (2015). *Information security in the workplace: A mixed-methods approach to understanding and improving security behaviours.* Unpublished doctoral dissertationUK: Northumbria University, Newcastle-upon-tyne.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees ' security behaviors. *Eleventh symposium on usable privacy and security (SOUPS 2015)* (pp. 103–122). USENIX Association.

Boer, H., & Seydel, E. (1996). Protection motivation theory. In M. Connor, & P. Norman (Eds.). *Predicting health behavior*. Buckingham: Open University Press.

Bowerman, B., & O'Connell, R. (1990). *Linear statistical models: An applied approach.* Boston: PWS-kent.

Branley, D., Covey, J., & Hardey, M. (2014). Online Surveys: Investigating social media use and online risk. *SAGE research methods cases*SAGE Publications, Ltdhttps://doi.org/10.4135/9781446273050135146666.

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

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself Online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly, 93*(2), 409–429. https://doi.org/10.1177/1077699016640224.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii international conference on system Sciences* (pp. 1–10). IEEE. https://doi.org/10.1109/hicss.2009.74.

CompTIA (2015). *Cyber secure: A look at employee cybersecurity habits in the workplace.* Retrieved from https://www.comptia.org/resources/cyber-secure-a-look-at-employee-cybersecurity-habits-in-the-workplace.

Coventry, L., Briggs, P., Blythe, J. M., & Tran, M. (2014). *Using behavioural insights to improve the public' s use of cyber security best practices.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf.

CPNI (2017). *Cyber insider.* Retrieved from https://www.cpni.gov.uk/insider-threat.

Crossler, R. E. (2010). Protection motivation Theory: Understanding determinants to backing up personal data. *43rd Hawaii international conference on system Sciences* (pp. 1–10). IEEE. https://doi.org/10.1109/hicss.2010.311.

Crossler, R. E., & Bélanger, F. (2014). An extended perspective on individual security Behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS - Data Base, 45*(4), 51–71. https://doi.org/10.1145/2691517.2691521.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring Your own device policies utilizing protection motivation theory bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209–226. https://doi.org/10.2308/isys-50704.

Cyberaware (2018). *Software and app updates.* Retrieved from https://www.cyberaware.gov.uk/software-updates.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security, 48*, 281–297. https://doi.org/10.1016/j.cose.2014.11.002.

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions. *International Journal of Human-computer Studies, 72*(2), 154–168. https://doi.org/10.1016/j.ijhcs.2013.10.003.

DCMS (2017). *Cybersecurity breaches survey.* Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

Demuth, J. L., Morss, R. E., Lazo, J. K., & Trumbo, C. (2016). The effects of past hurricane experiences on evacuation intentions through risk perception and efficacy beliefs: A mediation analysis. *Weather, Climate, and Society, 8*(4), 327–344. https://doi.org/10.1175/WCAS-D-15-0074.1.

Dipboye, R. L. (1977). A critical review of Korman's self-consistency theory of work motivation and occupational choice. *Organizational Behavior & Human Performance, 18*(1), 108–126. https://doi.org/10.1016/0030-5073(77)90021-6.

Fagan, M., Khan, M. M. H., & Buck, R. (2015). A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior, 51*, 504–519. https://doi.org/10.1016/j.chb.2015.04.075.

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x.

Forbes (2014). *The reputational impact of it risk.* Retrieved from https://www-935.ibm.com/services/multimedia/RLL12363USEN_2014_Forbes_Insights.pdf.

GetSafeOnline (2018). *Viruses & spyware.* Retrieved from https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/.

Getsafeonlineorg (2015). *Spam & scam email.* Retrieved from https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security, 17*(3), 276–289. https://doi.org/10.1108/09685220910978112.

Harris, M., & Schaubroeck, J. (1988). A meta-analysis of self-supervisor, self-peer, and peer-supervisor ratings. *Personnel Psychology, 41*(1), 43–62. https://doi.org/10.1111/j.1744-6570.1988.tb00631.x.
Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6.
Ifinedo, P. (2011). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007.
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001.
Information-age.com (2016). *28 years later: The malware landscape in 2016.* Retrieved from http://www.information-age.com/28-years-later-malware-landscape-2016-123462883/.
Inglesant, P., & Sasse, M. (2010). The true cost of unusable password policies: Password use in the wild. *In proceedings of the SIGCHI conference on human factors in computing systems* (pp. 383–392). . https://doi.org/10.1145/1753326.1753384.
Ion, I., Reeder, R., & Consolvo, S. (2015). "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. *In 2015 symposium on usable privacy and security* (pp. 327–346). USENIX Association.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behavior: An empircal study. *MIS Quarterly, 34*(3), 549–566.
Kirlappos, I., Parkin, S., & Sasse, M. (2015). *Shadow security as a tool for the learning organization.* ACM SIGCAS Computers and Society. Retrieved from http://dl.acm.org/citation.cfm?id=2738216.
Korman, A. K. (1970). Toward an hypothesis of work behavior. *Journal of Applied Psychology, 54*(1), 31–41. https://doi.org/10.1037/h0028656.
Lee, K., & Allen, N. J. (2002). Organizational citizenship behavior and workplace deviance: The role of affect and cognitions. *Journal of Applied Psychology, 87*(1), 131–142.
Lee, Y., & Kozar, K. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109–119. https://doi.org/10.1016/j.im.2008.01.002.
Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445–454. https://doi.org/10.1080/01449290600879344.
Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer Usage : A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.
MacKenzie, S. B., Podsakoff, P. M., & Ahearne, M. (1998). Some possible antecedents and consequences of in-role and extra-role salesperson performance. *Journal of Marketing, 62*(3), 87–98. https://doi.org/10.2307/1251745.
Maddux, J. E., & Rogers, R. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*, 46–479. Retrieved from http://www.sciencedirect.com/science/article/pii/0022103183900239.
Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., et al. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. *Annals of Behavioral Medicine, 46*(1), 81–95. https://doi.org/10.1007/s12160-013-9486-6.
Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6*(1), 42. https://doi.org/10.1186/1748-5908-6-42.
Microsoft (2015). *Updating software help.* Retrieved from http://www.microsoft.com/security/portal/mmpc/help/updateFAQs.aspx.
Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*(2), 163–184. https://doi.org/10.1348/135910702169420.
Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health related behaviour: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x.
Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. *Proceedings of the annual Hawaii international conference on system Sciences* (pp. 3188–3197). . https://doi.org/10.1109/HICSS.2014.396.
Nappa, A., Johnson, R., Bilge, L., Caballero, J., & Dumitraş, T. (2015). The attack of the clones: A study of the impact of shared code on vulnerability patching. *Proceedings - IEEE symposium on security and privacy, 2015–July* (pp. 692–708). . https://doi.org/10.1109/SP.2015.48.
National Cyber Security Centre (2017). *Password Guidance: Simplifying Your approach.* Retrieved from https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach.
Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010.
Organ, D. (1988). *Organizational citizenship behavior: The good soldier syndrome.* Lexington, MA: Lexington Books.
Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure.* Suny Press.
Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly, 31*(4), 623–656.
Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology, 7*(1), 84–107. https://doi.org/10.1037/1089-2680.7.1.84.
Podsakoff, P. M., & MacKenzie, S. B. (1997). Impact of organizational citizenship behavior on organizational performance: A review and suggestion for future research. *Human Performance, 10*(2), 133–151. https://doi.org/10.1207/s15327043hup1002_5.
Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.
Podsakoff, N. P., Whiting, S., Podsakoff, P. M., & Blume, B. (2009). Individual-and organizational-level consequences of organizational citizenship behaviors: A meta-analysis. *Journal of Applied Psychology, 94*(1), 122–141. https://doi.org/10.1037/a0013079.
Ponemon Institute (2015). *2015 cost of data breach Study: Global analysis.* Retrieved from http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF.
Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803.
Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.). *Social psychophysiology: A sourcebook* (pp. 153–176). New York: Guilford Press.
Sans (2015). *Glossary of security terms - Z.* Retrieved from http://www.sans.org/security-resources/glossary-of-terms/?pass=z.
Seccomglobal (2017). *WANNA.CRY. why was this cyber attack so damaging?* Retrieved from https://www.seccomglobal.com/white-papers/wanna-cry-cyber-attack-damaging/.
Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046.
Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.
Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security Policies: An empirical investigation. *Computer, 43*(2), 64–71. https://doi.org/10.1109/MC.2010.35.
Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045.
Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security, 23*(2), 200–217. https://doi.org/10.1108/ics-04-2014-0025.
Symantec (2014). *Malicious links: Spammers change malware delivery tactics.* Retrieved from http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics.
Symantec (2016). *Latest intelligence for october 2016.* Retrieved from https://www.symantec.com/connect/blogs/latest-intelligence-october-2016.
Symantec (2017). *Advanced persistent Threats: How they work.* Retrieved from https://www.symantec.com/theme.jsp?themeid=apt-infographic-1.
Telegraph (2016). *TalkTalk loses 101,000 customers after hack.* Retrieved from http://www.telegraph.co.uk/technology/2016/02/02/talktalk-loses-101000-customers-after-hack/.
Van Steen, T. (2017). *Susceptibility to influence briefing Note: Analysis of cyber security campaigns*.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002.
Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy Compliance: The role of Autonomy and efficacy. *Journal of Information Privacy and Security, 9*(4), 52–79. https://doi.org/10.1080/15536548.2013.10845690.
Williams, S. L., & French, D. P. (2011). What are the most effective intervention techniques for changing physical activity self-efficacy and physical activity behaviour–and are they the same? *Health Education Research, 26*(2), 308–322. https://doi.org/10.1093/her/cyr005.
Witte, K., Cmaeron, K., McKeon, J., & Berkowitz, J. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 4*(1), 317–341. https://doi.org/10.1080/108107396127988.
Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the Twenty–Sixth International Conference on Information Systems,* 367–380.
Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005.
Zhang, L., & McDowell, W. C. (2009). Am I really at Risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3–4), 180–197. https://doi.org/10.1080/15332860903467508.
Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330–340. https://doi.org/10.1108/09685220910993980.