2018-06-01

Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior

Clarke, N

10.1108/ICS-03-2018-0037
Information and Computer Security
Emerald

Emerald Information Management and Computer Security

Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior

Journal:	*Information and Computer Security*
Manuscript ID	ICS-03-2018-0037
Manuscript Type:	Original Article
Keywords:	Information security modeling, Risk analysis

Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior

Abstract

Purpose - The end-user has frequently been identified as the weakest link; however, motivated by the fact that different users react differently to the same stimuli, identifying the reasons behind variations in security behavior and why certain users could be "*at risk*" more than others is a step towards protecting and defending users against security attacks. This paper aims to explore the effect of personality trait variations (through the Big Five Inventory (BFI)) on users' risk level of their intended security behaviors. In addition, age, gender, service usage and IT proficiency are also analyzed to identify what role and impact they have towards behavior.

Design/methodology/approach – The authors developed a quantitative-oriented survey that was implemented online. The Bi-variate Pearson Two-tailed Correlation was used to analyze survey responses.

Findings - The results obtained by analyzing 538 survey responses suggest that personality traits do play a significant role in affecting users' security behavior risk levels. Further to that, the results suggest that BFI score of a trait has a significant effect as users online personality is linked to their offline personality especially in the conscientiousness personality trait. Additionally, this effect was stronger when personality was correlated with the factors of IT proficiency, gender, age and online activity.

Originality/value – The contributions of this paper are two-fold. First, with the aid of a large population sample, end-users' security practice is assessed from multiple domains and relationships were found between end-users' risk-taking behavior and 9 user-centric factors. Second, based upon these findings, the predictive ability for these user-centric factors were evaluated to determine the level of risk a user is subject to on an individual behavior perspective. Of 28 behaviors, 11 were found to have a 60% or greater predictive ability, with the highest classification of 92% for several behaviors. This provides a basis for organizations to utilize behavioral intent alongside personality traits and demographics to understand and, therefore, manage the human aspects of risk.

Key Words Personality Traits, BFI, Security behavior, Risk, Correlation

Paper Type Research paper

1. Introduction

People around the world rely heavily on the Internet and its services for carrying out their everyday activities. This is evident as most homes have one or more computing device connected to the Internet where more than 3.8 billion users use the Internet in 2017 compared to 2.9, 3.1 and 3.4 billion in 2014, 2015 and 2016 respectively (InternetLiveStats, 2017). With this growing Internet popularity, comes an increase in information security threats such as social engineering, hacking and malware. Regardless of the common use of security methods to protect IT systems, such as biometrics and antivirus software, the threat landscape is continuously revolving. For instance, more than 7.1 billion identities were exposed in data breaches since 2010 which is equivalent to one for every person in the world. More than 1.1 billion identities were exposed in 2016 compared to over 563 million in 2015 (almost the double). In these data breaches, the percentage of lost financial information such as credit or debit card details was 32.9% in 2015 and increased by 10% to 42.9 in 2016 (Symantec, 2017). However, costs of such breaches can extremely damage businesses and individuals with an average cost to business from $38,000 to $551,000 (Kaspersky, 2015).

Attackers are constantly increasing their efforts to create sophisticated malware and hacking methods. Technology alone has been found not enough to ensure the protection of IT systems as it can be misused by end-users and, thus, losing its usefulness (Kaur and Mustafa, 2013; Furnell and Moore, 2014). As such, the way how security attacks are formed has changed intensively from being mainly carried out technically to focusing upon the weakest link in information security domain, i.e the end-user (Dhillon and Backhouse, 2000; Schneier, 2000; Siponen, 2000; Wade, 2004). From the attacking perspective, cyber-attacks such as spam, phishing and ransomware that require end-users' involvement, by clicking on them for example, are widely spreading. This is apparent as the rate of email malware has increased from 1 in 220 and 1 in 244 in 2014 and 2015 respectively to 1 in every 131 emails in 2016 while the number of detected ransomware jumped from 340,665 in 2015 to 463,841 in 2016 (Syamntec,

2017). Unfortunately, this may cost individuals an average of $700 per ransomware incident (statista.com). Whereas from the defending perspective, a number of surveys suggest that organizations have huge concerns about their employees regarding cyberattacks (FBI, 2015) especially that employees mistakes are considered one of the top threats to information security in organizations (Rao and Pati, 2012; Hansch and Benenson, 2014). IBM's 2015 Cyber Security Intelligence Index suggests that 95% of cyber security breaches within organizations are due to human error (IBM, 2016). Within the UK, for example, 75% of enterprises and 31% of SMBs suffer staff-related security incidents (PwC, 2015). Moreover, Kaspersky's IT Security Risks Survey suggests that staff are responsible for 29% and 21% of unintentional and intentional data leaks respectively (Kaspersky, 2014). Simultaneously, research studies have also demonstrated that malicious/careless insiders are the main threat to business's IT systems (Pfleeger and Caputo, 2012; Posey et al., 2011).

Identifying the characteristics that may influence user's security behavior and being highly vulnerable to security threats is an important step in protecting and defending users against security attacks. Additionally, as users intentions may differ from their actual behavior and the fact that different users react differently to the same stimuli (Egelman and Peer, 2015), it is imperative to understand the extent in which users are practicing good security behavior and the reasons behind these variations in security practices. Therefore, knowing how this behavior is influenced by user differences and to what extent, will help in designing solutions that adapt to the needs of those who are vulnerable. Early studies mainly focus upon obtaining end-users' perception on various topics. For instant, several research papers, such as Florêncio *et al.* (2014), Stobert and Biddle (2014), and Wash *et al.* (2016), investigated end-user's password usage; also studies, including Canfield *et al.* (2016), Jain and Gupta (2016), Singh *et al.* (2011) focused upon end-user related phishing attacks. Although these studies demonstrate various cases of end-users' security practice (or at least behavioral intent) and highlight areas that should be focused to reduce the risk and hence to improve the IT security, they are often lack in providing the reason that end-users exhibit certain security behavior. Recently, studies have sought to explore the field further by exploring factors that may influence users' security practice. Kruger *et al*. (2011) studied the impact of cultural factors (e.g., language and field of study) upon end-users' awareness levels and security behavior. Also, Sheng *et al*. (2010) investigated the relationship between phishing susceptibility and end-users' demographic factors (e.g., age and gender); and, Halevi *et al.* (2013), Kajzer *et al*. (2014), and Shropshire *et al*. (2015) explored the connection between end-users' personalities (e.g., openness and conscientiousness) with their security activities. However, these studies are somewhat limited in terms of the number of user security activities, participants, and/or factors being considered. Therefore, this paper investigates the relationship between end-users' security practices from multiple domains (i.e., 28 questions on authentication, email security, security software usage, and data management) and 9 user-centric factors including the personalities through the BFI, demographics, IT proficiency and IT usage. Using this understanding of behavioral intent, personality and demographics, the study develops and evaluates a predictive model that seeks to understand an end-user's security risk. This understanding can be subsequently incorporated within organizational security planning/risk management to aid in managing risk.

The remainder of the paper is structured as follows: Section 2 reviews related studies on the factors affecting end-users' security practice. Sections 3 and 4 present the research methodology and results of the survey study. The correlation between end-user security practice, their personalities and several other user-oriented factors is presented in Section 5. Section 6 presents a model to predict risk based upon the aforementioned variables; and conclusions and future work are highlighted in Section 7.

2. Related Work

It is widely observed that end-users practice IT security differently; and those who exercise bad IT security actions would put the IT system into a more risky situation than those who carry out good IT security behaviors. It is inevitable that end-users will behave differently due to their varied factors (e.g., backgrounds and experiences). If the reason why end-users exhibit certain behavior could be learnt,

adequate strategies (e.g., customized IT security training program) can then be developed and hence the overall IT security can be improved. With the aim of investigating the relationship between end-users' characteristics and their IT security practices, a number of survey studies have been designed and conducted. An analysis of these studies is presented as follows.

2.1 Demographic factors

Demographics, include age, gender, education level, and occupation, are the most common characteristics that are often used to analyze behaviors. For example, the password is the most common protection method for end-users' systems and data. Bonneau (2012) has demonstrated that the strength of the password is associated with end-users' age (i.e., older users tend to use more complex password) and their nationalities. Schuessler and Hite (2014) suggest that a user's password strength is affected by their educational background and work ethic. Butler and Butler (2014) undertook a survey of 737 respondents to explore other factors have suggested that poor password behavior could be caused by the lack of user's knowledge and motivation. From the attacking perspective, social engineering is a simple yet effective attack that is widely used to obtain end-users' information, such as login credentials. Workman (2007) demonstrates that social engineering victims shared several common factors (e.g., age, education, and commitment). Also, Sheng *et al.* (2010) suggest that gender and age are two key indicators that can be used to predict end-users' phishing susceptibility as they found that female participants aged 18-25 were more vulnerable to phishing attacks. From a training and education perspective, Jeske *et al*. (2014) suggest that a user's IT proficiency was in line with their security decisions; and hence better security decisions can be made if user's IT proficiency was improved. By studying the impact of cultural factors on user's security awareness levels, Kruger *et al*. (2011) demonstrate that the user's security awareness levels are related with their language, gender and fields of study.

2.2 Personality factors

Personality is the "combination of characteristics or qualities that form an individual's distinctive character" (Oxford English Dictionary, 2016); and the use of personality to understand user's behavior is a well-established domain. In order to obtain a person's personality characteristics, a number of test models can be utilized, such as the Revised NEO Personality Inventory (Costa and McCrae, 1992), Five-Factor Model Rating Form (Lynam and Widiger, 2001), and Ten-Item Personality Inventory (Gosling et al 2003). Amongst these models, John and Srivastava's (1999) 44-item Big Five Inventory (BFI) model is one of the most widely accepted and used across several research domains. The BFI model contains 5 main set of personality traits: extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience (Costa and McCrae, 1992). The use of personality factors to predict and explain various IT security behavior was initially proposed by Shropshire *et al*. (2006). However, they only theoretically discussed the ability of two personalities (i.e., conscientiousness and agreeableness) to predict user's IT security compliant behavior. Since then, several research works have been conducted in this area. Based upon empirical results, Gabriel and Furnell (2011) demonstrate that 8 personality facets show strong correlation with end-user's generic security behavior, for example, imagination facet and user's security behavior have positive correlation while the immoderation facet and user's security behavior have a negative correlation. Schuessler and Hite (2014) suggest that both agreeableness and neuroticism are negatively related with user's password strength while extroversion shows a positive correlation. Shrophire *et al*. (2015) claim that the connection between user's behavioral intent and use of security software can be moderated by agreeableness and conscientiousness; while Uffen *et al*. (2013) investigated the influence of personality upon smartphone users' opinions upon the effectiveness of security mechanisms specifically. Their experimental results suggested that both openness and conscientiousness have positive correlation upon user's intentions to utilize smartphone security controls while neuroticism has a negative one. Kajzer *et al.* (2014) suggest that a best fit security awareness theme can be introduced based upon user's personality, hence, potentially improving the user's IT security proficiency. For the attacking perspective, a couple of studies have investigated the impact of personality upon end-users' behavior on phishing emails. Halevi *et al.* (2013) demonstrate that a high

correlation was found between the neuroticism and responding to phishing attacks. Meanwhile, Pattinson *et al.* (2012) show that openness, extraversion, and agreeableness were related with user's actions when dealing with the same situation. From the Organisational point of view, a number of studies demonstrated some evidence that personalities can influence security policy compliance (Herath and Rao, 2009; Hu *et al*. 2012; McBride *et al*. 2012; Johnston *et al*. 2016) and potential insider misuse (Warkentin *et al*., 2012).

2.3 Discussion

Prior work on investigating the relationship between various factors and user's security behaviors is already established; and a summary of existing studies is presented in Table 1. Nonetheless, a number of limitations are observed from these studies, including the low number of participants (e.g., Kruger *et al*. (2011) and McBride *et al.* (2012)) and factors being considered mainly focused on demographics (e.g., Workman (2007). Moreover, Gabriel and Furnell (2011) concentrated on personalities only while Hu *et al*. (2012) targeted on the impact of top management and organizational culture. Additional limitations are limited user security behaviors (e.g., phishing (Sheng *et al.*, 2010) and password practice (Schuessler and Hite, 2014). Therefore, a study that investigates the relationship between end-user security behavior and differentiating factors from a holistic perspective would provide a deeper insight into variety of affecting factors and risk taking behavior.

Studies	Focus	Outcomes	Method	No. of participants
Workman, 2007	Investigates reasons why people may fall victim of social engineering attacks	Results demonstrate social engineering victims share several common factors (including age, education, and trust)	Regression	588
Herath and Rao, 2009	Assess the impact of organization's commitment upon employee's intentions with security compliance	Suggest that self-efficacy is a strong indicator of user's intentions regarding policy compliance	Correlation and a component-based approach of Partial Least Square (PLS)	312
Sheng *et al*., 2010	Investigate the relationship between phishing susceptibility and demographics	Both gender and age can be used to predict a user's weakness in phishing	Multivariate linear regression	1001
Kruger *et al*., 2011	Study the impact of culture in user's IT security awareness	Mother tongue has an impact on security awareness level	ANOVA test	180
Gabriel and Furnell, 2011	Investigate the connection between user's security behavior and their personalities	8 personality facets showing strong correlation with user's security behavior	Pearson correlation	20
Hu *et al*., 2012	Investigate a number of factors on how to manage employee to comply with InfoSec policies	Demonstrate that conscientiousness has a significantly positive effect on the user's intention on InfoSec polices compliance	A component-based approach of PLS	148
McBride *et al*., 2012	Investigate the impact of situational factors and personality traits upon policy violation within the InfoSec domain	Confirms that users respond to same security scenarios different due to their personality traits	General linear mixed model analysis	150
Pattinson *et al*., 2012	Study whether personalities have impact on how people mange phishing emails	When dealing with phishing emails, openness and extraversion are associated with not-informed users while agreeableness is related with informed users.	Spearman's correlation	117
Warkentin *et al*., 2012	An investigation of individual personalities on insider abuse intentions	Their results confirm that personalities have impacts upon individual's cybersecurity behavior	Random Intercept Model	86
Halevi *et al*., 2013	Study how user's personality traits contributed to their cyber security and privacy practice	The correlation between the neurosis trait and user's responding to phishing attacks is high	Bi-variate Pearson correlation	100
Uffen *et al*., 2013	Explore the influence of personality has upon smartphone users' opinions on the effectiveness of a security mechanism	Their outcomes indicate that some personalities influence how security controls are used by the user	A component-based approach of PLS	435
Jeske *et al*., 2014	Explore the relationship between IT proficiency, impulse control and secure behavior	Self-judged IT proficiency was in line with secure decisions; greater impulse issues are more likely to make poorer security decisions	Covariates Regression	67
Kajzer *et al*., 2014	Investigate effectiveness of various InfoSec awareness messages upon users according to their personalities	Their exploratory results suggest that practitioners can be assisted in finding a more suitable way to tailor security awareness messages according to users' personality profiles.	Regression	293
Schuessler and Hite, 2014	Explore the relationship between several factors (e.g., personality and work ethics) and the strength of password chosen by users.	The user's password strength were related with their personality and work ethic	t-test, 2-tailed, and 1-tailed	71
Shropshire *et al*., 2015	Investigate the impact of personality upon user's security software usage	Agreeableness and conscientiousness have strong relation with whether users would use security software	A components-based structural equation modeling	170
Johnston *et al*., 2016	Study the impact of dispositional and situational factors upon violations on InfoSec policy	Their results suggest that the connection between situational factors and security policy violation can be moderated by using dispositional factors	A generalized form of the standard linear model	242

Table 1: Existing work on investigating the relationship between various demographic and personality factors and user's security behaviour

3. Methodology

With the aim to investigate the relationship between various user factors (including personalities) and their security behavior[1], the following research questions (RQ) were created:

RQ1: "*What is the general risk level associated with a user's security behavior*?"

RQ2: "*Is there a relationship between user's factor X and the risk level of security behavior y*"

RQ3: "*If there is a relationship between user's factor X and the risk level of security behavior y, how strong is that relationship*"

To obtain meaningful responses to the proposed research questions, a quantitative-oriented survey was devised, enabling generic statistical models (e.g., Pearson's correlation) to be applied on the response. The survey contains 28 main questions that are organized as follows: demographics, general IT usage, IT proficiency, IT security practice and the BFI personality test. Demographics are used to establish an understanding of respondent's background and along with the personality section provide the factors to compare behavior against. General IT usage is utilized to obtain an understanding of type and level of technology and services use. IT security practice is designed to understand the level of risk (i.e., high, medium and low) associated with end-user's security behavior from a number of domains, such as authentication and network management. The personality test is employed to appreciate different user's personality traits via the 44-item Big Five Inventory model of John and Srivastava (1999).

After obtaining an ethical approval from the authors' institution, the survey was implemented online via the LimeSurvey tool. With the aim of maximizing the number of participants, invitations were distributed to students and colleagues of the authors via emails and social networking websites. In total, 563 completed responses are gathered. However, 538 participants' responses are selected for the analysis as the other 25 participants answered wrongly to at least one of controlled questions and their responses are removed completely from the study.

4. Survey Findings

An analysis of the demographic questions from the 538 responses was initially conducted. Regarding gender, age, education, and IT proficiency, the data is skewed towards men (71%), 18-35 (77%), with a degree (68%) and experienced in IT (80%). This was somewhat expected due to the authors availability and access to participants. However, it was notable that 53% participants are non-IT professionals. Despite this phenomenon does not weaken the results, it is important to highlight the participants' usage in technology and/or their security behavior would be higher than the ones from the general population. Based upon the results from prior studies, this also suggests they are likely to exhibit better security behaviors than one would expect from a wider population.

4.1 Use of Technology and Services

The way end-users utilize IT technology and services could offer several indicators to potential security threats upon their information; obviously the more they use, the higher chance their information could be open to abuse if security controls are not correctly utilized. As shown in Figure 1, participants' top three used technologies are Windows desktop/laptop (81%), iPad/iPhone (75%), and Android based tablet/smartphone (54%); in contrast, only 6.9% and 4.1% of the surveyed used BlackBerry based devices and smartwatches respectively. As expected, this result is in line with current trends (Net Applications, 2016). More notably, 65% of the participants use three or more devices, suggesting users and their information could be misused from multi directions; in addition, this would require end-users to learn more on security in order to maintain their devices and data safe.

[1] Whilst the term security behavior is utilized throughout this paper, in all cases unless otherwise specified, this refers to behavioral intent rather than actual behavior.

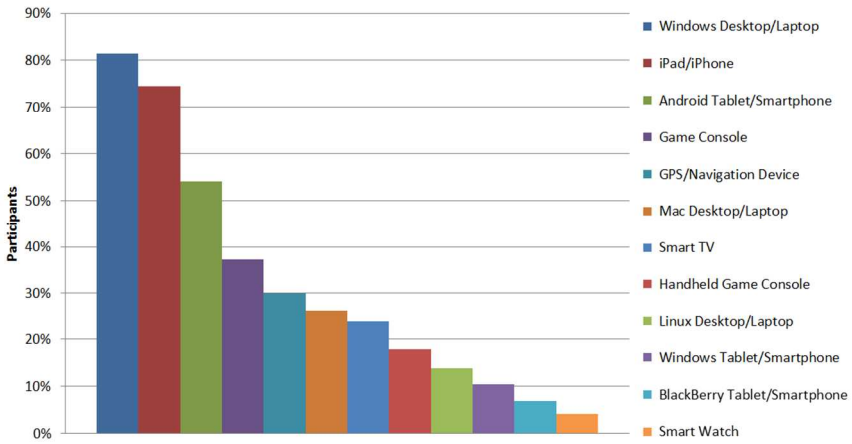

Figure 1. End-users' Technology Usage

In addition to their device usage, participants' usages on online services were also examined. Based upon how frequently they use these services, three levels of usage are obtained: high (i.e., *always*), medium (i.e., *often*), and low (i.e., *sometimes, rarely and never*). As illustrated in Figure 2, email is the most popular service as 77% of the participants had a high usage; in addition, office applications, instant messenger, online streaming, and social networking are also very popular as more than 70% of the participants claimed that they use these services on at least *often* basis. Continuing the trend of analyzing concurrent use, 87% of surveyed have access to minimum 5 services at a high/medium basis, suggesting majority of the participants highly engage with different IT technology and services.

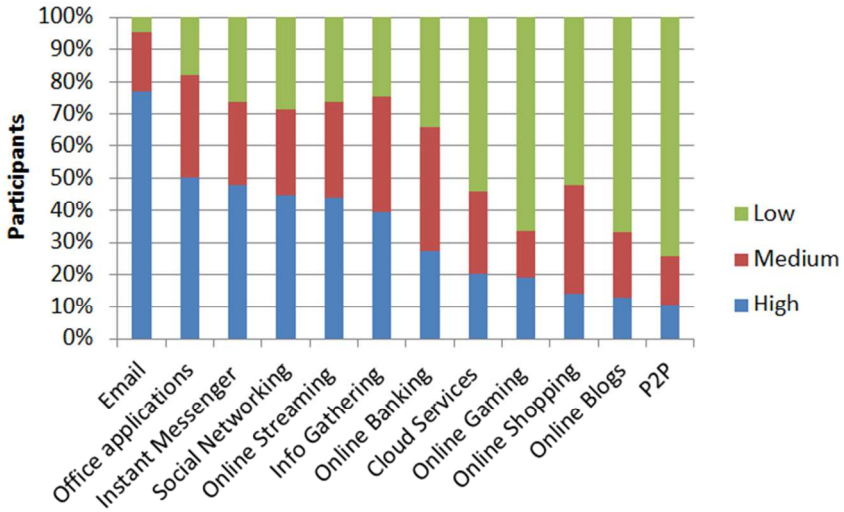

Figure 2. End-users' Usage on various IT Services

4.2 Risk Level of End-User Practice

In terms of IT security, 27% and 47% of the participants considered it as essential and a high priority accordingly; this result is encouraging as almost three quarters of the participants highlighted the importance of security within their mindsets. It is envisaged that they would practice better security than those considered IT security is less important. Also, 88% of surveyed have prior experience with security incidents, such as infected by malware and loss of data. As a result, arguably these end-users should be able to protect their devices and data better in comparison with those had little prior knowledge about dealing with incidents. . To estimate the level of risk associated with their security practice, participants are initially asked how often they perform an activity, i.e., *always*, *often*, *sometimes*, *rarely*, and *never*; which were then codified into three risk levels (i.e., high, medium, and low) based upon the types (i.e.,

positive and negative) of the security activity. For the positive security activity (e.g., a user scans a USB drive before using it), the more frequent the user performs it, the lower the risk level is associated to it. Therefore, for the positive security activities, "*always*" is coded into low; "*often*" is coded into medium; and "*sometimes*, *rarely* and *never*" are coded into high. In comparison, for the negative security activity (e.g., a user stores his/her passwords), the more frequent the user does it, the higher the risk level is linked to it. As a result, "*always*, *often*, and *sometimes*" are coded into high; "*rarely*" is coded into medium; and "*never*" is coded into low for the negative security activities. According to this, the risk level of end-user's practice is assessed from several areas, including password usage, application usage, and network management.

4.2.1. Password Hygiene

The password is the most used authentication method that is used to protect end-user's system and information. As a result, it is important that end-users use their passwords in a secure manner. Nevertheless, 46.3% of participants have less than 6 passwords for all their services and devices, providing a strong indication of password reuse as 98.1% of the surveyed use 10 services and/or devices or more. Despite the use of a strong password is effective to protect systems from password cracking attacks, more than four fifths of the participants' passwords were poorly created (e.g. less than eight characters in length and does not contain a symbol. Also, less than two thirds of the participants change their passwords regularly (i.e., within a 6-month timeframe); and 42.2% of the participants only change their passwords if they were asked (e.g., a system may force its users to change their password every 6 months), providing a large window of opportunity for attackers if a user's password is compromised.

Other areas that are used to evaluate the risk level of password practices include password sharing, storing, and reusing. As illustrated in Figure 3, the best password security practice amongst the chosen categories is password sharing: 61.3% of the participants have low risk as they *never* shared their passwords with others; a similar result is presented in Helkala and Bakas (2013) that 63% of their 1,003 users do not share their passwords. Unfortunately, the results also highlight that almost two fifths of users have experience of sharing their passwords, demonstrating that an opportunity exists for a high level of misuse on IT systems and data. In comparison, password re-usage is associated with the highest level of risk as 63.2% of the participants claim they frequently use the same password for multiple sensitive accounts and about two thirds of the participants store their passwords. These practices offer opportunities to attackers who can obtain access to multiple systems by only successfully hacking into one of the systems. Similar trends are observed on saved password on browsers/systems and logging off from online systems activities – less than one quarter of the participants practice them safely. It is envisaged that both activities offer some levels of user convenience (e.g., saving time) and users have less concerns as these browsers/online systems are initially protected by the main OS authentication mechanism (assuming it is correctly used). In contrast, participants appreciate the role of the password for workstations as more than two thirds of them often lock their stations when they are away from desks. Based upon these results, it shows that significant effort is required on reducing the risk of password practice even for users with a more technical savvy and educated background. Password practice activities that are associated with high risk levels are also linked to user convenience: system security is compromised as user convenience is more preferred. Therefore, additional consideration regarding usability and security should be given by designers when developing new systems.

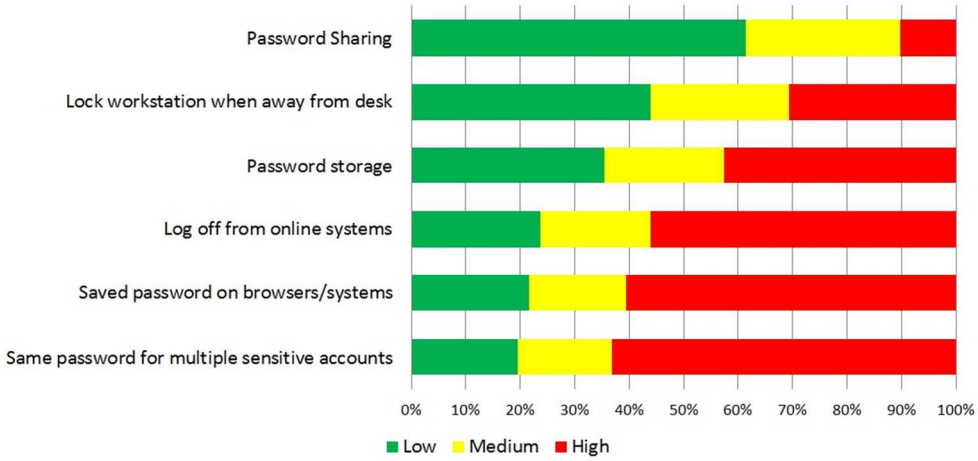

Figure 3. The risk level of user password security practice

4.2.2 Software Security

In order to keep the IT system safe, it is important that end-user's activities on their systems and applications can be learned. One common security practice is to update systems/applications regularly as a range of vulnerability could exist in unpatched software. As illustrated in Figure 4, just over half of the participants always update their antivirus software. While the other half of the participants put their IT systems into a more risky environment as an adequate level of protection cannot be provided by antivirus software with out-of-date signatures. Indeed, Microsoft's biannual Security Intelligence Report suggests that the infection rate of Windows OSs with out of date security software is more than three times higher than those with latest signatures (Microsoft, 2014). Regarding general applications (e.g., web browsers), two thirds of the participants delay the security related patch installation for their software, endangering their systems, with 85% of exploitation attacks related to unpatched software (i.e., posing medium to high risks to their systems) (Canadian Cyber Incident Response Centre, 2015). Interestingly, these results also show a similar pattern that is obtained from the password practice in terms of user convenience. Regarding anti-virus software update, the burden upon the end-user is removed as the process is typically configured as automated. Conversely, the end-user's attention is more required for patching: either to approve it or to wait whilst an automated patch is installed, and often more inconveniently a reboot of the system could be required.

Other good software security practices also include not disabling antivirus/firewall and avoiding illegal software as the former provides basic protections against malware and network intrusions while the latter highly likely contains Trojans or backdoors. Nonetheless, 41.4% of the surveyed have disabled antivirus software/firewall on their devices before; and the survey data suggests that similar proportion of participants (42.4%) frequently utilize pirate software (i.e., posing high risks to their systems). Further analysis reveals that a quarter of the total participants perform activities on both chosen criteria; yet 72% of them claimed that they are experienced and expert IT users. This phenomenon could suggest that while technical users understand better security they may also be the ones who put the IT systems at a higher risk.

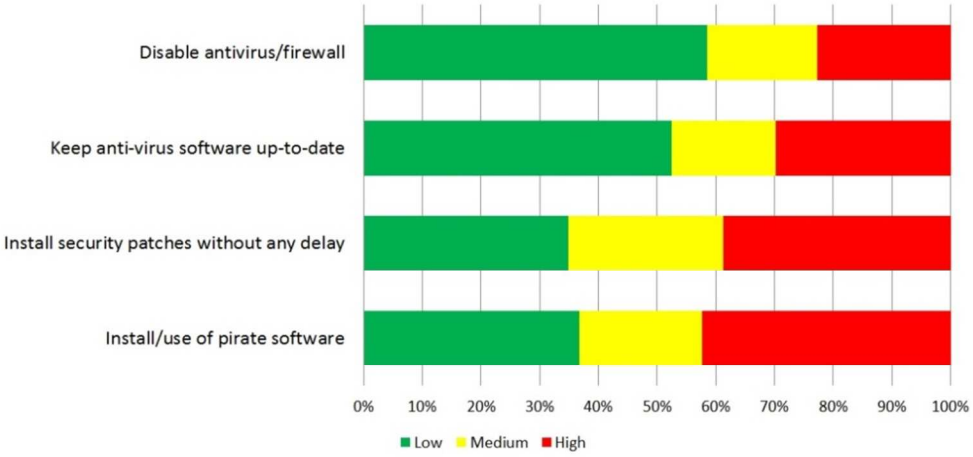

Figure 4. The risk level of user software security practice

4.2.3 Email Security

As demonstrated earlier, email is the most of popular application that is used by end users. Nevertheless, its popularity also poses a number of threats as cybercriminals often use it to launch various attacks (e.g., spam, phishing, and malware) (Symantec, 2016). For phishing alone, a total of 687,964 unique phishing email campaigns are reported to the Anti-Phishing Working Group (APWG) in the first three months of 2016 (APWG, 2016). As shown by Figure 5, almost two thirds of the participants claim that they *never* click on links/attachments if the email was sent by someone they do not know; in comparison only 28.4% would take the same action when the message was sent by their colleagues/friends, highlighting the importance of trust and also potential danger when the sender's email was perpetrated. In terms of treating suspicious emails, participants' behavior is good in general as three quarters of the surveyed claim to delete them. Spam, which chain emails are a form of, is also an increasing threat to email users (Kaspersky 2015). The majority of participants were knowledgeable of such emails, as evidenced by almost 70% never forwarding them. However, 72.1% of the participants *never* notify IT support about suspicious emails although such warning could benefit other end-users from being victimized; despite the reason for such user behavior is unclear at this stage, this could be due to the frequency of such attacks and/or the lack end-users awareness.

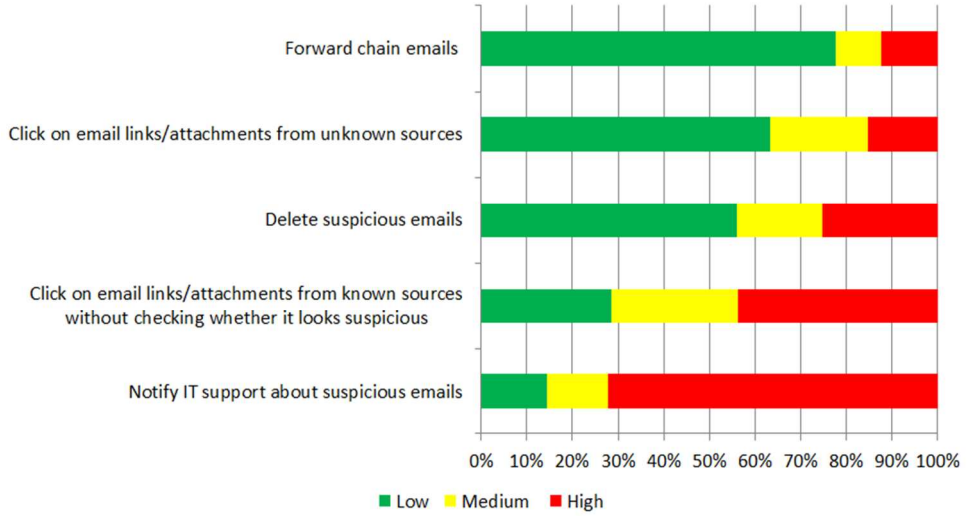

Figure 5. The risk level of user email security practice

4.2.4 Data Management

Good data management is essential for the security of IT systems as legitimate data are often critical and sensitive while illegitimate data may contain malicious codes. If it is not properly handled, legitimate data may be misused; while illegitimate data could be a source of threat for IT systems.

Regarding user's data security, backup is a long-established solution against incidents such as loss of data or malicious data modification; while encryption can be used to protect confidential information. It is always good practice to use both methods to ensure the data's confidentiality, integrity and availability. Nevertheless, 72.7% of participants do not regularly backup their data, posing them to medium to high risks (as demonstrated in Figure 6). While the usage of encryption for their data is even less convincing: only 6.5% of participants *always* use encryption when transferring data via a USB drive and 11.3% claimed they *always* encrypt sensitive information that is stored on their computer. Conversely, when disposing of information, participants seem to be more aware, with two thirds of the participants regularly destroying their data before disposing of hardware.

In order to protect their IT system from various attacks, end-users should practice better security on data, such as paying more attention to security warnings and data from unknown sources, and scanning a USB drive before usage. More than four fifths of the participants have used a USB drive without scanning and open a document despite security warnings. Both activities are associated with potential embedded malware/Trojans, hence posing medium to high level of risks. In comparison, users are more careful when dealing with data from unknown sources. As illustrated by Figure 6, over one third of the participants *never* access USB/downloading files from unknown sources; as a result, very little risks are presented in their activities.

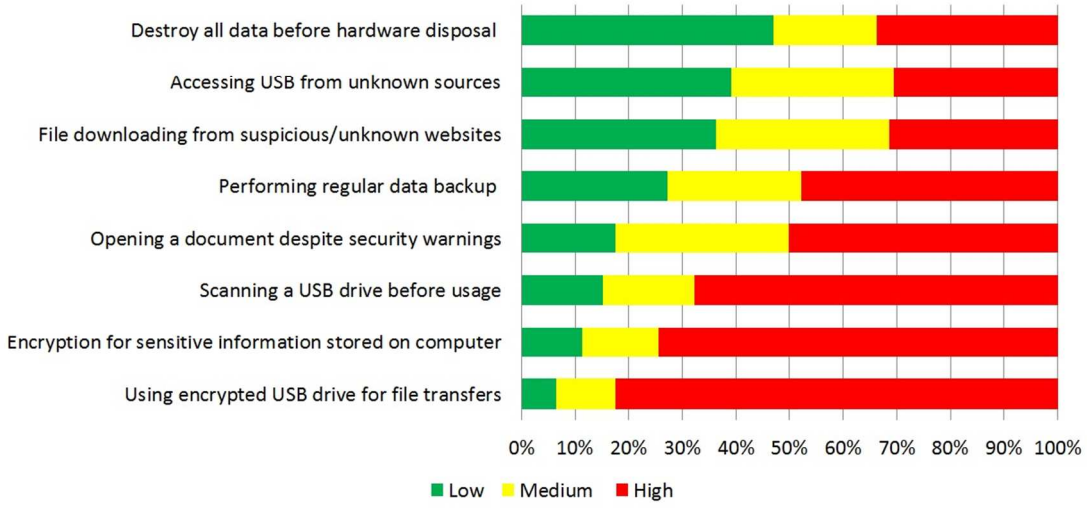

Figure 6. The risk level of user data management practice

4.2.5 Network Management

Good network management is essential to protect devices and its data against various network related attacks (e.g. browser attacks and man-in-the-middle attack). It is common practice that network security managers and IT administrators are responsible for securing business networks and servers. However, it is mainly individual's responsibility to protect their own endpoints.

A Virtual Private Network (VPN) enables end-users to connect to a private network and access information over public networks securely. Figure 7 shows that less than 5% of the participants utilize the service on an 'always' basis (i.e. low risk level). This could be because VPN technology is mainly used to access corporate networks and the participants were largely recruited within academic environment that is less business focused. However, users do have more control over the use of wireless technology on their devices. The security issue and privacy concern over using public Wi-Fi network and disabling wireless technologies when not using them are well documented (Potter, 2006; Zafft and Agu, 2012; Cheng *et al*., 2013; Wright and Cache, 215); however, more than 90% and 80% of participants still do not securely practice them respectively. The use of an anonymizing proxy or the TOR network is a for (from user's point of view) and against (from system administrator's standing point) area in terms of security and privacy. Nevertheless, the survey result shows that less than one third of the participants *always* use the technique for anonymous communication.

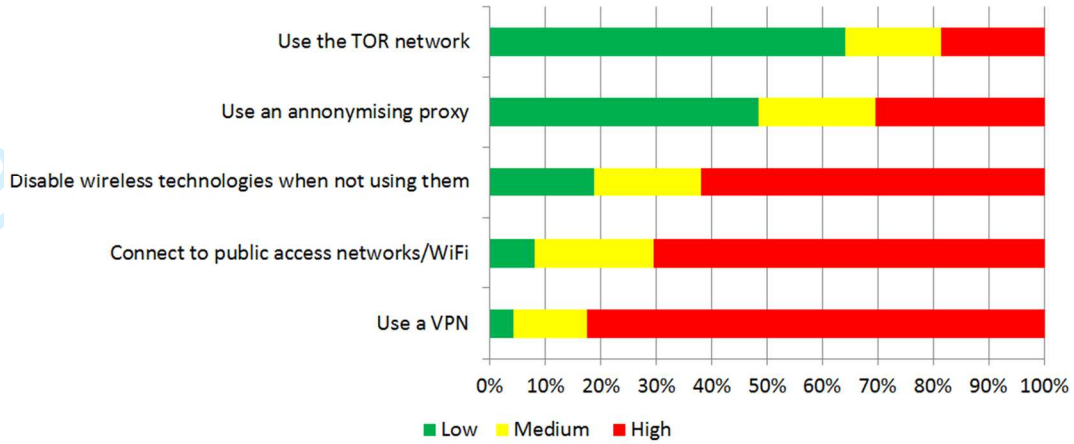

Figure 7. The risk level of user network management practice

5. Significance Testing on the relationship between user factors and the risk taking behavior

With the aim of exploring the relationship between various user-oriented factors and the risk level of their intended security behaviors, the survey data was examined using the Bi-variate Pearson two-tailed correlation. The correlation output of the risk level across 28 security behaviors and 9 user-centric factors (including personalities and demographics) is presented in Table 2.

Amongst the personality factors, *conscientiousness* is negatively correlated with the risk of most user security behaviors (19 out of 28 are highly significant (i.e., p-value of 0.01) and 3 are significant (i.e., p-value of 0.05)). This appears logical as people who score high on the *conscientiousness* scale have been shown to be more responsible (Zhang, 2006). A similar trend can also observed from the *agreeableness* and *openness* personality factors; both are negatively correlated with the user's security behavior/risk level. The former and the latter are associated with 10 and 12 behaviors at a significant level respectively. In comparison, the *neuroticism* factor is positively correlated with the user's security behavioral risk level: with 7 behaviors being statistically significant. This suggests people with high *neuroticism* are likely to be emotional more unstable; as a result, their security behavior might be more radical than others. With respect to *extraversion*, only one of the security behaviors correlated with significance. This suggests it is not a suitable moderator for predicting the risk level associated with user's security behavior.

Investigating the demographic factors, age is negatively related with the risk level of more than half of the end-user's security behaviors (i.e., 10 are highly significant and 6 are significant), suggesting the younger a user is, the higher the risk. One of the reasons behind this could be the more mature a person is, the more responsible they are. This is confirmed from a further analysis on the survey data that shows age and conscientiousness are positively correlated ($r=0.158^{**}$, $p=0.01$). Regarding gender, the results demonstrate very little significance, with only the odd behavior flagging as significant.

Regarding the self-judged factors (i.e., IT proficiency and service usage), a general trend of negative correlation between end-user's security behavioral risk level and their factors is demonstrated by the results. The higher score of a factor, the lower the risk level associated to it. The results are almost self-explanatory: the higher the user's IT skill level and their familiarity with IT services, the lower the risk level is associated with their behaviors as they tend to understand more about IT services and would take IT security more seriously. Nonetheless, five positive correlations (representing less than one third of total significant correlations) are presented between the service usage and the security behaviors, including Install/use of pirate software, Opening a document despite security warnings, and Saved password on browsers/systems. The first two could suggest that users with a high level of understanding of IT tend to be more arrogant when dealing certain IT risks; while the last one could be caused by the amount of additional/repeated authentication that is often required for high usage users.

N=538	BFI					Demographics		Self-judged	
Security Behavior	E	A	C	N	O	Age	Gender	IT Proficiency	Service Usage
Password Sharing	.091*	0.000	-.163**	0.047	-0.074	-0.071	-.181**	-.168**	-0.046
Lock workstation when away from desk	-0.063	-0.031	-.188**	-0.003	-0.069	-.106*	0.031	-.148**	-.156**
Password storage	0.020	-0.070	0.009	-0.009	-.088*	0.0034	-.098*	-.119**	-0.007
Log off from online systems	-0.052	-0.072	-.182**	.090*	-.118**	-.092*	-0.051	-0.060	0.070
Saved password on browsers/systems	0.013	-0.070	-.173**	0.054	-0.005	-.191**	0.035	0.051	.238**
Same password for multiple sensitive accounts	0.037	0.030	-.129**	.096*	-.092*	-.220**	-0.056	-.257**	0.046
Disable antivirus/firewall	-0.061	-.112**	-.212**	0.081	-.116**	-.097*	-0.015	-.209**	-0.063
Keep anti-virus software up-to-date	-0.013	-0.070	-.222**	.097*	-.099*	-.093*	-.109*	-.355**	-.205**
Install security patches without any delay	-0.001	-.101*	-.176**	.147**	-.114**	-0.083	-.206**	-.278**	-.229**
Install/use of pirate software	0.005	-.123**	-.159**	0.056	-0.050	-.311**	.174**	0.005	.138**
Forward chain emails	0.034	-.186**	-.178**	0.082	-.130**	-0.048	-0.012	-.197**	-.116**
Click on email links/attachments from unknown sources	-0.016	-.098*	-.159**	0.075	-.128**	-0.001	-.114**	-.212**	-.120**
Delete suspicious emails	-0.022	-.095*	-.100*	0.057	-.103*	-.204**	0.059	-.113**	-0.069
Click on email links/attachments from known sources without checking whether it looks suspicious	0.006	-0.063	-.095*	0.042	-0.079	-0.009	-.124**	-.224**	-.097*
Notify IT support about suspicious emails	-0.033	-0.024	-0.071	0.046	-0.041	-.271**	0.080	0.000	-0.068
Destroy all data before hardware disposal	0.007	-.116**	-.141**	.094*	-.150**	-.124**	-.095*	-.231**	-.161**
Accessing USB from unknown sources	0.005	-0.070	-.132**	0.057	-0.035	-0.016	-0.033	-.168**	-0.048
File downloading from suspicious/unknown websites	-0.034	-.163**	-.193**	.114**	-0.057	-.185**	0.047	-0.012	0.013
Performing regular data backup	-0.073	-0.054	-.243**	0.072	-0.069	-.188**	0.068	-.212**	-.165**
Opening a document despite security warnings	-0.016	-.153**	-.187**	0.061	-0.056	-.262**	0.022	0.005	.133**
Scanning a USB drive before usage	-0.046	-0.034	-.145**	.119**	-.113**	-0.083	-.128**	-0.062	-.117**
Encryption for sensitive information stored on computer	-0.072	-0.046	-0.053	0.075	-0.068	-0.049	-.113**	-.137**	-.111*
Use encrypted USB drive for file transfers	-0.067	-0.065	-0.055	-0.006	-0.023	-0.065	0.063	0.035	0.004
Use the TOR network	-0.059	-.097*	-0.053	0.030	-0.01	-.103*	.138**	-0.004	0.055
Use an anonymising proxy	-0.071	-0.071	-.133**	0.040	-0.023	-.137**	.232**	0.062	.158**
Disable wireless technologies when not using them	0.008	-0.012	-.096*	-0.017	-0.083	0.048	-.134**	-0.072	-0.053
Connect to public access networks/Wi-Fi	0.051	-0.045	-0.028	0.038	-0.046	-.105*	-0.076	-.091*	.143**
Use a VPN	0.031	0.028	-0.028	-0.031	-.104*	-0.076	-0.064	-0.082	-.131**

Table 2. Pearson Correlation results on various user's factors and the risk level of their security behaviors

E: Extraversion; A: Agreeableness; C: Conscientiousness; N: Neuroticism; O: Openness; *. Correlation is significant at the 0.05 level (2-tailed).**. Correlation is significant at the 0.01 level (2-tailed).

6. A Model to Predict Risk based upon Behavior, Age, Gender and IT Proficiency

The survey results and correlation analysis has shown and reaffirmed that users are still undertaking risky decisions across a range of security-related behaviors – even acknowledging the skew within the population sample which would suggest participants exhibiting better rather than poorer security behavior. The significance testing in particular has assisted in identifying the specific relationship between behaviors and various user-oriented factors. Whilst this is both relevant and interesting, the ability to use this knowledge in a proactive manner and individualized manner could help organizations in managing and mitigating their risk posture from a people perspective. For example, predicting an individual's risk-taking behavior during recruitment could help ensure an organization has the right mixture of employees. Alternatively, better understanding individuals could also enable organizations to provide more targeting training or put in place increased monitoring.

As such, an investigation was undertaken to explore the extent participants risk taking behavior could be predicted. Furthermore, the experiment sought to understand which of the user-oriented factors would be more useful in the prediction. To achieve this, a neural network-based classification approach was utilized, with each behavioral question resulting in a separate network. A feature vector based upon a selection of user-oriented factors was then applied. A supervised pattern recognition feedforward neural network was utilized due to its ability to approximate to any polynomial function – and this provides the necessary scope to derive the necessary decision boundaries (Andoni *et al*., 2014). The 538 respondents were randomly split into 300 for training and 238 for testing and the experiment was repeated ten times to reduce the variability introduced in the random weight assignment in the neural network. Results were then averaged across the ten runs.

As illustrated in Table 3, 12 of the 28 behaviors can be predicted with an accuracy of 60% or better, with the most accurate prediction of 92% (for the use of anonymized proxy and TOR behaviors). An analysis across the groups of behaviors found 4 out of 5 sections contained at least one highly predictive behavior. Only the software security set of behaviors did not find result in an accurate prediction. These relationships were largely consistent across the differing feature vectors generated from the user-oriented factors, with marginally better results being predicted using just the BFI.

Security Behaviour	Feature Vector		
	BFI	BFI, Age, IT proficiency	All Features
Password Security Practice			
Password Sharing	**51%**	**50%**	**52%**
Lock workstation when away from desk	**41%**	39%	39%
Password storage	**40%**	34%	37%
Log off from online systems	**58%**	**57%**	**53%**
Saved password on browsers/systems	**61%**	**61%**	**61%**
Same password for multiple sensitive accounts	**67%**	**66%**	**61%**
Software Security			
Disable antivirus/firewall	**44%**	**43%**	**44%**
Keep anti-virus software up-to-date	36%	**40%**	**40%**
Install security patches without any delay	31%	**41%**	**42%**
Install/use of pirate software	**45%**	34%	**43%**
Email Security			
Forward chain emails	**64%**	**63%**	**64%**
Click on email links/attachments from unknown sources	**49%**	**48%**	**49%**
Delete suspicious emails	**48%**	**48%**	**45%**
Click on email links/attachments from known sources without checking whether it looks suspicious	34%	29%	31%

Notify IT support about suspicious emails	**69%**	**67%**	**67%**
Data Management			
Destroy all data before hardware disposal	**42%**	**45%**	**47%**
Accessing USB from unknown sources	31%	31%	32%
File downloading from suspicious/unknown websites	35%	35%	36%
Performing regular data backup	**49%**	**40%**	**40%**
Opening a document despite security warnings	**49%**	**49%**	**45%**
Scanning a USB drive before usage	**66%**	**69%**	**67%**
Encryption for sensitive information stored on computer	**74%**	**75%**	**75%**
Use encrypted USB drive for file transfers	**79%**	**78%**	**78%**
Network Management			
Use the TOR network	**92%**	**92%**	**92%**
Use an annonymising proxy	**92%**	**92%**	**92%**
Disable wireless technologies when not using them	**62%**	**63%**	**62%**
Connect to public access networks/Wi-Fi	**80%**	**79%**	**78%**
Use a VPN	**80%**	**80%**	**80%**

Table 3. Prediction of User Risk

7. Conclusion and Future Work

The study has sought to further investigate the relationship between user's behavior (or specifically behavioral intent) and various user-oriented factors. A more complete set of analyses across a wider set of behaviors and factors has provided a more appreciable understanding of what significant relationships exist. *Conscientiousness, agreeableness* and *openness* all play a role across two-thirds of all behaviors. The study has also reaffirmed that age and self-claimed proficiency (both IT and usage) also have an impact on behavior.

Capitalizing upon this knowledge, a predictive model has experimental shown it is possible to use these user-oriented factors in predicting the risk-taking behavior an individual will partake in. Using this model, it is anticipated that organizations can better select, train and monitor personnel – enabling them to incorporate a meaningful and manageable risk profile for employees. Further research will also focus upon how to capitalize upon this to provide end-users with more effective awareness based upon the risks they present to systems.

References

Andoni, A., Panigrahy, R., Valiant, G., and Zhang, L. (2014), "Learning polynomials with neural networks", In *Proceedings of the 31st International Conference on Machine Learning (ICML-14)*, pp. 1908–1916

APWG (2016), "Phishing Activity Trends Report", available at: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf (accessed 20 March 2017)

Bonneau, J. (2012). ,"The Science of Guessing Analyzing an Anonymized Corpus of 70 Million Passwords", *IEEE Symposium on Security and Privacy*, San Francisco, California.

Butler, R. and Butler, MJ (2014), "An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers", in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA, 2014)*, 8-10 July, Plymouth UK, pp150-161

Canadian Cyber Incident Response Centre (2015), "Top 4 Strategies to Mitigate Targeted Cyber Intrusions", available at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx (accessed 20 March 2017)

Canfield, C.I, Fischhoff, B. and Davis, A. (2016),"Quantifying Phishing Susceptibility for Detection and Behavior Decisions", *Human Factors*, Vol.58 No.8, pp. 1158 – 1172

Cheng, N., Wang, X., Cheng, W., Mohapatra, P. and Seneviratne, A. (2013), "Characterizing privacy leakage of public WiFi networks for users on travel", in *Proceedings IEEE INFOCOM*, Turin, 2013, pp. 2769-2777

Costa, P. T., Jr., & McCrae, R. R. (1992), "*Revised NEO Personality Inventory (NEO PI-R) and NEO Five-Factor Inventory (NEO-FFI) professional manual*", Odessa, FL: Psychological Assessment Resources.

Dhillon, G., and Backhouse, J. (2000), "Information System Security Management in the New Millennium", *Communications of the ACM*, Vol. 43 ,pp.125-128.

Egelman, S. and Peer, E. (2015), "The Myth of The Average User: Improving Privacy and Security Through Individualization ", In: *Proceedings of the 2015 New Security Paradigms Workshop NSPW'15, Twente, Netherlands*, ACM, pp. 16-28

Evans, J. D. (1996), *Straightforward statistics for the behavioral sciences*, Pacific Grove, CA: Brooks/Cole Publishing

FBI (2015), "2015 Internet Crime Report", available at: https://pdf.ic3.gov/2015_IC3Report.pdf (accessed 03 March 2017)

Florêncio, D., Herley, C. and van Oorschot, P.C. (2014), "An Administrator's Guide to Internet Password Research", in *Proceedings of the 28th Large Installation System Administration Conference*, November 9-14, Seattle, US, pp.35-52

Furnell, S. and Moore, L. (2014), "Security literacy: the missing link in today's online society?", *Computer Fraud & Security*, Vol.5, pp.12-18

Gabriel, T. and Furnell, S. (2011),"Selecting security champions", *Computer Fraud & Security*, Vol.8, pp.8-12

Gosling, S.D, Rentfrow, P.J and Swann, W.B. (2003), "A very brief measure of the Big-Five personality domains", *Journal of Research in Personality*, Vol.37 No.6, pp. 504–528.

Halevi, T., Lewis, J. and Memon, N. (2013), "A Pilot Study Of Cyber Security And Privacy Related Behavior And Personality Traits", in *International World Wide Web Conference (IW3C2) in Rio de Janero, Brazil*, ACM, pp.737-744

Helkala, K. and Bakas, T.H. (2013), "National Password Security Survey: Results", in *Proceedings of the European Information Security Multi-Conference (EISMC 2013) in Lisbon, Portugal*, University of Plymouth Press, pp23-24

Hansch, N. and Benenson, Z. (2014), " Specifying IT security awareness", In: *25th International Workshop on Database and Expert Systems Applications*, IEEE, pp.326 - 330.

Herath, T. and Rao, H. (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

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences*, Vol.43 No.4, pp.615–660.

IBM (2016), "2015 Cyber Security Intelligence Index", available at: http://www-01.ibm.com/common/ssi/cgibin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF (accessed 11 January 2017)

InternetLiveStats (2017), "Internet users", available at: http://www.internetlivestats.com/internet-users/ (accessed: 15 February 2018)

Jain, A.K and Gupta, B.B. (2016), "A novel approach to protect against phishing attacks at client side using auto-update white-list", *EURASIP Journal on Information Security*, Vol.2016 No.9, pp. 1-11

John, O. P., and Srivastava, S. (1999), "The Big-Five trait taxonomy: History, measurement, and theoretical perspectives", In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research*, Guilford Press, New York, pp. 102-138

Johnston, A., Warkentin, M., McBride, M. and Carter, L. (2016), "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems,* Vol.25 No.3, pp.231‑251

Kajzer, M., D'Arcy, J., Crowell, C., Striegel, A. and Van Bruggen, D. (2014), "An Exploratory Investigation Of Message-Person Congruence In Information Security Awareness Campaigns", *Computers & Security*, Vol. 43, pp.64-76

Kaspersky (2014), "IT Security Risks Survey 2014", available at: http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf (accessed 10 May 2017)

Kaspersky (2015), "Global IT security Risks Survey", available at: http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf (accessed: 03 April 2017)

Kaur, J. and Mustafa, N. (2013), "Examining the effects of knowledge, attitude and behavior on information security awareness: A Case on SME", In *3rd International Conference on Research and Innovation in Information Systems (ICRIIS'13) in Kuala lumpur, Malaysia*, IEEE, pp.286 - 290.

Kruger, H., Flowerday, S., Drevin, L. and Steyn, T. (2011), "An Assessment Of The Role Of Cultural Factors In Information Security Awareness". in *(ISSA) Information Security South Africa* in *Johannesburg*, *South Africa*, IEEE, pp.1 – 7

Lynam, D. R. and Widiger, T. A. (2001), "Using the five-factor model to represent the DSM-IV personality disorders: An expert consensus approach", *Journal of Abnormal Psychology*, Vol.110 No.3, pp.401–412.

Microsoft (2014), "Microsoft Security Intelligence Report", Volume 17, available at: https://www.microsoft.com/security/sir/archive/default.aspx (accessed: 19 October 2016)

Net Applications (2016), "Operating System Share", available at: http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=9&qpcustomb=0 (accessed: 20 December 2016)

Oxford English Dictionary (2016), "Personality", available at: https://en.oxforddictionaries.com/definition/personality (accessed 16 November 2016)

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. (2012),"Why do some people manage phishing e-mails better than others?", *Information Management & Computer Security*, Vol. 20 No.1, pp. 18 – 28

Pfleeger, S. and Caputo D. (2012), "Leveraging behavioural science to mitigate cyber security risk", *Computers & Security*, Vol. 31 No.4, pp. 597-611

Posey, C., Bennett, R and Roberts, T. (2011), "Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes", *Computer & Security*, vol.30 No.6, pp. 486-497

Potter, B. (2006), "Wireless Hotspots: Petri Dish of Wireless Security", *Communications of the ACM*, Vol.49 No.6, pp. 51–56.

PwC (2015), "2015 Information Security Breaches Survey", available at: http://www.pwc.co.uk/assets/pdf/2015-ISBS-Technical-Report-blue-digital.pdf (accessed: 18 February 2017)

Rao, U. and Pati, B. (2012), "Study of Internet security threats among home users", In: *Fourth International Conference on Computational Aspects of Social Networks, Sao Carlos, Brazil*, IEEE, pp.217 - 221.

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, New York

Schuessler, J.H. and Hite, D.M. (2014), "Pre-Employment Screening for Security Risk: An Exploratory Study", *Journal of Applied Business and Economics*, Vol. 16 No.1, pp. 84-9

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. and Downs, J. (2010), "Who Falls For Phish? A Demographic Analysis Of Phishing Susceptibility And Effectiveness Of Interventions", in Proceedings of the *CHI Conference on Human Factors inComputing Buisness in Atlanta, Georgia, USA*, ACM, pp. 373 – 382

Shropshire, J., Warkentin, M., Johnston, A. C., & Schmidt, M. B. (2006), "Personality and IT security: An application of the five-factor model", in *Proceedings of the Americas Conference on Information Systems AMCIS in Acapulco, México*, pp.3443-3449

Shropshire, J., Warkentin, M. and Sharma, S. (2015), "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security*, Vol.49, pp.177-191.

Singh A.P., Kumar V., Sengar S.S., and Wairiya M. (2011), "Detection and Prevention of Phishing Attack Using Dynamic Watermarking", In: Das V.V., Thomas G., Lumban Gaol F. (eds) *Information Technology and Mobile Communication. Communications in Computer and Information Science*, Vol. 147. Springer, Berlin, Heidelberg

Siponen, M.T. (2000), "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice", *Information Management & Computer Security*, Vol. 8, pp. 197-209

Stanton, J.M., Stam, K.R., Mastrangelo,. And Jolton, J. (2005), "Analysis of end user security behaviours", *Computers & Security*, Vol. 24, 2005, pp. 124-133.

Stobert, E. and Biddle, R. (2014), "The password life cycle: user behaviour in managing passwords", *in Proceedings of the Tenth Symposium on Usable Privacy and Security, Menlo Park, CA, USA*, ACM, pp. 243-255

Symantec (2017), "Internet Security Threat Report", Volume 22, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (accessed 20 December 2016)

Wade, J. (2004), "The Weak link in IT Security", *Risk Management*, Vol.51 No.7, pp. 32-37

Warkentin, M., McBride, M., Carter, L. and Johnston, A. "The Role of Individual Characteristics on Insider Abuse Intentions", in *Proceedings of the 18th Americas Conference on Information Systems in Seattle, Washington*, USA, Association for Information Systems (AIS), pp. 4833-4842

Wash, R., Rader, E. and Wellmer, Z. (2016), "Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites", in *proceedings of the Twelfth Symposium on Usable Privacy and Security, in Denver, USA* , ACM, pp.175-188

Workman, M. (2007), "Wisecrackers: a theory grounded investigation of phishing and pretext social engineering threats to information security", *Journal of the American Society of Information Science and Technology*, Vol.59, pp. 662–674

Wright, J. and Cache, J (2015), *Hacking Exposed Wireless: Wireless Security Secretes & Solutions*, third edition, McGraw-Hill Education, New York, USA

Uffen, J., Kaemmerer, N, and Breitner, M.H. (2013), "Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures", *Journal of Information Security*, Vol.4, pp. 203-212

Zafft A. and Agu E. (2012), "Malicious WiFi networks: A first look", *37th Annual IEEE Conference on Local Computer Networks – Workshops* in *Clearwater, FL, USA*, IEEE, pp. 1038-1043

Zhang, L. (2006), "Thinking styles and the big five personality traits revisited", *Personality and Individual Differences,* Vol.40 No.6, pp.1177-1187.