Heliyon

*Received:*
2 May 2017
*Revised:*
9 June 2017
*Accepted:*
29 June 2017

Cite as: Lee Hadlington. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3 (2017) e00346. doi: 10.1016/j.heliyon.2017.e00346

# Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours

**Lee Hadlington** *

*De Montfort University, Leicester LE1 9BH, UK*

* Corresponding author.

E-mail address: lhadlington@dmu.ac.uk (L. Hadlington).

## Abstract

The present study explored the relationship between risky cybersecurity behaviours, attitudes towards cybersecurity in a business environment, Internet addiction, and impulsivity. 538 participants in part-time or full-time employment in the UK completed an online questionnaire, with responses from 515 being used in the data analysis. The survey included an attitude towards cybercrime and cybersecurity in business scale, a measure of impulsivity, Internet addiction and a 'risky' cybersecurity behaviours scale. The results demonstrated that Internet addiction was a significant predictor for risky cybersecurity behaviours. A positive attitude towards cybersecurity in business was negatively related to risky cybersecurity behaviours. Finally, the measure of impulsivity revealed that both attentional and motor impulsivity were both significant positive predictors of risky cybersecurity behaviours, with non-planning being a significant negative predictor. The results present a further step in understanding the individual differences that

http://dx.doi.org/10.1016/j.heliyon.2017.e00346

may govern good cybersecurity practices, highlighting the need to focus directly on more effective training and awareness mechanisms.

Keywords: Psychology

## 1. Introduction

In 2010 the British Government assigned the growing threat from Cybercrime a "Tier One" status, its highest level of concern (HMSO, 2010). In the same year, a report published by The Symantec Corporation (LaBrie et al., 2010) noted that globally, 65% of adults had fallen victim to some form of cybercrime. The economic cost of breaches in cybersecurity has also been noted, with an estimated cost of between £75,000 and £311,000 for small and medium-sized enterprises (SMEs), this figure rising to between £1.46 m and £3.14 m for larger organisations (HM Government, 2015). The current research is presented alongside this alarming rise in cybercrime. The key aim is to provide an exploration of how individual differences serve to influence employee's engagement in information security behaviours.

Human factors in the context of information security has begun to gain increased attention, particularly where the use of security technologies have failed to protect companies from cyberattacks (Anwar et al., 2016; Herath and Rao, 2009a, b). The use of such technologies is negated in instances where employees fail to follow cybersecurity protocols or engage in activities that place themselves and the company at risk. It is from this perspective that the growth in research exploring the role human factors play in information security has been born (Herath and Rao, 2009b). Research has found that employees consistently underestimated the probability of falling victim to a cybersecurity breach (Herath and Rao, 2009a). Herath and Rao (2009b) further argued that organisational, environmental and behavioural factors all serve to influence the extent to which employees adhere to cyber security practices.

### 1.1. Personality traits and cybersecurity

Some attempts have been made to explore how individual differences in personality traits can impact on a person's adherence to cybersecurity procedures. For example, Shropshire, Warkentin, Johnston, and Schmidt (2006) initially proposed a link between the intent to comply with information security protocols and the traits of agreeableness and conscientiousness. McBride et al. (2012) also noted that individuals who are more extraverted were more likely to violate cybersecurity polices in comparison to more neurotic and conscientious individuals. Shropshire et al., 2015 found that the intent to use a new piece of security software and actual use was also mediated by conscientiousness and agreeableness. However it should be noted that this last piece of research focused


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

on a cohort of students aged between 18–21, potentially limiting the extension of these findings to a work-based population. The researchers also noted a general discrepancy between behavioural intent and actual behaviour, further exacerbating the capacity to predict security compliant behaviours (Shropshire et al., 2015).

Additional work exploring the link between personality traits and susceptibility to attacks has been included in pioneering work by Uebelacker and Quiel, (2014). This work examined the link between susceptibility to social engineering attacks and key personality factors. Social engineering is viewed as the use of manipulation, persuasion, and influence by an attacker to obtain sensitive information or access to restricted areas (Uebelacker and Quiel, 2014). Uebelacker and Quiel, (2014) presented a theoretical framework based on a comprehensive literature review that made direct links between the Big Five Personality traits (see John and Srivastava, 1999) and susceptibility to social engineering. The authors suggested that individuals exhibiting traits such as conscientiousness, extraversion, openness to experience, and agreeableness were highly susceptible to social engineering attacks. In contrast, further studies exploring information security behaviours have noted that conscientiousness, agreeableness and openness to experience were linked to lower risk taking and higher information security awareness scores (McCormac et al., 2016). This discrepancy in findings further highlights the potential benefits of conducting more research to examine the impact aspects of personality have on information security behaviours.

One personality trait that has been focused on within the research surrounding information security behaviours is that of impulsivity. Impulsiveness has been defined as "the urge to act spontaneously without reflecting on an action and its consequences" (Coutlee et al., 2014; p. 2). Research has shown that individuals who exhibit higher levels of impulsivity are less risk adverse when compared to those with lower levels (Coutlee et al., 2014; McCoul and Haslam, 2001; Zuckerman and Kuhlman, 2000). Coutlee et al. (2014) also noted trait impulsivity is a component of a wide number of clinical conditions such as ADHD, borderline personality disorder and impulsive control disorders. Recent work has also established links between impulsivity and aspects of information security awareness. For instance Egelman and Peer (Egelman and Peer, 2015b) explored the link between impulsivity and information security using their own Security Behaviours Intentions Scale (SeBIS). This scale examined awareness and engagement in good cybersecurity practices, including the use of different passwords for different accounts, verifying the authenticity of links before they follow them and keeping software up-to-date. Findings from this research showed that impulsivity was negatively correlated to security behaviours, presenting the potential for this trait to predict risky cybersecurity behaviours.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Welk et al. (2015) assessed the impact of individual differences on participant's capacity to discriminate between legitimate emails and phishing emails. A phishing email typically involves some form of social engineering tactic with the attacker purporting to be an official source in an attempt to elicit personal information such as account login details (Welk et al., 2015). Welk et al. (2015) noted that measures of personality and impulsivity acted as significant predictors of detecting a phishing email. Individuals who scored higher on measures of extraversion and anxiousness performed significantly poorer on detecting phishing emails. Aspects of impulsivity including reservation, calmness, and the capacity to keep emotions under control were also positively correlated with the accuracy in detecting phishing emails. Those who were rated as being more reserved, calmer and have the capacity to keep their emotions in check had better detection rates for phishing emails (Welk et al., 2015).

Tischer et al. (2016) examined the potential for individuals to plug in USB devices that had been littered around a university campus. This process is often seen as a key mechanism of infiltration used by social engineers who will leave such devices in prominent places in an attempt to gain entry to highly protected systems (Tischer et al., 2016). Often such devices will be laden with malicious software allowing the social engineer remote access to system once they have been plugged into a computer connected to the Internet. In contrast to Egelman and Peer's work, Tischer et al. (2016) found that individuals who were more likely to plug in a USB device were no more risk loving when compared to a matched sample. In fact those individuals who did plug in the USB were more risk averse in all categories apart from that of recreational risk. It does appear that these individuals devolve responsibility for their protection to the computer and security measures deployed on it, or are ignorant of the risks attached to poor cybersecurity practices (Tischer et al., 2016). Tischer et al. (2016) also used the SeBIS, but noted that the internal reliability of the scale was found to be much lower than had originally been found in the original research by Egelman and Peer (2015b). As there appears to be a lack of clarity in the research literature about the impact trait impulsivity has on both attitudes and behaviours in the context of information security, the present research aimed to examine this further. It is proposed, based on the previous findings from research, that impulsivity will significantly predict adherence to information security protocols.

## 1.2. Internet addiction and computer abuse

Internet addiction has garnered a great deal of attention over the past two decades, with many arguing for it to be classified as a pathological disorder. (Griffiths, 1998; Griffiths, 2000; Young, 1998). Griffiths (2000) suggested that the concept of *Internet* addiction is potentially a misnomer, and is an umbrella term that actually masks other technological addictions fuelled by access to the Internet. These could


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

include aspects of addiction to email (Marulanda-Carter and Jackson, 2012), online gaming (Kuss et al., 2012; Ng and Wiemer-Hastings, 2005), and social networking (Karaiskos et al., 2010).

To date there have been no explicit attempts to link Internet addiction to the potential to engage in risky cybersecurity behaviours. Most of the research examining the impact of Internet addiction in the workplace has focused on aspects of lost productivity (Greenfield and Davis, 2002; Young and Case, 2004). A potential link between Internet addiction and Internet abuse has been mention in the research literature, with Griffiths (2010) noting that although related, these concepts are not the same. Stanton (2002) previously made the suggestion that Internet abuse in the workplace is a natural extension of activities related to Internet addiction. Accordingly, Rosen (2010) claimed that the new iGeneration of workers believe that they have the right to be online at all times, irrespective of if they are in work or not. Aspects of Internet abuse are not without an associated cost, and can lead to the clogging of computer networks as well as increasing the incidents of security breaches within an organisation (Pee et al., 2008; Weatherbee, 2010). Chen et al. (2008) noted that unethical use of the Internet within the workplace had the potential to develop into cybercrime, including aspects of intellectual property theft, distributing offensive material and online piracy. Panko (2010) also noted that users could cause a variety of issues through computer abuse and misuse, such as inadvertently downloading malicious code or visiting compromised websites. Further work is deemed necessary to establish exactly how aspects of technology addition link into poor cybersecurity behaviours and in turn if such a metric could be used to help organisations target training more effectively. It is suggested that those individuals exhibiting a compulsive use of the Internet will be inclined to take more risks in order to get online, and as a result be less compliant with accepted protocols.

## 1.3. Aims and objectives

The focus for this study is to explore if trait impulsivity, Internet addiction and attitudes of employees towards cybersecurity serve to predict the frequency of engaging in risky cybersecurity behaviours. The inclusion of an attitude scale serves to act as a metric against which the behaviour of individuals can be examined, as well as providing the capacity to measure change over time. From this regard, the attitude scale has the potential to be particularly useful when exploring the impact intervention strategies have on knowledge and awareness of cybersecurity within a variety of settings. By concentrating on those individuals in employment it is hoped that findings could be used to develop strategies to prevent lapses in business cybersecurity. The current study will also explore the potential for individual differences in impulsivity and Internet addiction to act as predictors for risky cybersecurity behaviours. Building on the research reviewed above the


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

tentative suggestion is that Internet addiction and impulsivity will act as significant positive predictors for more frequent engagement in risky cybersecurity behaviours. In the instance of attitudes towards cybersecurity, it is suggested that a negative attitude towards cybersecurity and cybercrime in business will be associated with to higher levels of risky cybersecurity behaviours.

## 2. Methods

### 2.1. Participants

Participants were recruited via an online questionnaire using Qualtrics Research Panel, and were paid a small honorarium for their participation. In total a total of 538 participants completed the survey, with an age range of 18 – 84, comprising of 218 Males and 297 Females. All participants were in employed work (either Part-Time or Full-Time) and based in the UK.

### 2.2. Materials

#### *2.2.1. Abbreviated impulsiveness scale (ABIS)*

A shortened 13-item impulsivity scale presented by Coutlee et al. (2014) was used to counter the potential for participant response fatigue. Items are scored on a scale of 1 (Never/Rarely) to 4 (Almost Always/Always), with possible scores ranging from 13–52. The ABIS consists of three sub-scales, namely Attention, Motor and Non-planning. Coutlee et al. (2014) reported Cronbach's α of 0.80, 0.82, and 0.71 respectively for each of these sub-scales.

#### *2.2.2. Online cognition scale (OCS)*

Davis et al. (2002) presented a 36-item scale that is designed to explore aspects of excessive Internet Use. The scale has exhibited a high level of internal consistency with a Cronbach's α of 0.94. Scores on the OCS range between 36 and 252, with the upper level being indicative of problematic Internet use.

#### *2.2.3. Risky cybersecurity behaviours scale (RScB)*

Partially based on the SeBIS (Egelman and Peer, 2015a, b) a scale was created with input from Digital Forensic investigators and Law Enforcement. It included behaviours that had led to companies being attacked as a result of poor cybersecurity practices. The questionnaire asked participants to rate, on a scale of 0–6 (where 0 = Never and 6 = Daily), how often they engaged in the specific behaviour during a previous 6-month period. Items included 'Sharing passwords with friends and colleagues', 'Using the same password for multiple websites', and 'Using an online storage system to exchange and keep personal or sensitive information'. The final scale included 20 items, with possible scores ranging from


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

0–150. Higher scores on the RScB were indicative of the individual engaging in more risky cybersecurity behaviours. In the present study, for the 20-item scale an overall Cronbach's α of 0.823 was achieved, indicating a high level of reliability. The full list of items for this scale is shown in Table 1.

### 2.2.4. Attitudes towards cybersecurity and cybercrime in business (ATC-IB)

The scale was constructed to reflect a wide spectrum of attitudes towards both cybersecurity and cybercrime within a business context. The scale was constructed using expertise from the Police, Digital Forensics, Criminal Psychology and Cyberpsychology. A final scale consisting of 25 items was used in the study and consisted of items such as *'I don't have the right skills to be able to protect the organisation from cybercrime*'. The scale was scored using a 4-point Likert scale; (4) Strongly Disagree, (3) Disagree, (2) Agree, (1) Strongly Agree. A high score on the ATC-IB scale indicated a positive engagement in cybersecurity, where as a lower score indicated a negative attitude and lower engagement. Scores on the

**Table 1.** Scale Items for the Risky Cybersecurity Behaviours Scale (RScB).

| | Item |
|---|---|
| 1 | Sharing passwords with friends and colleagues. |
| 2 | Using or creating passwords that are not very complicated (e.g. family name and date of birth). |
| 3 | Using the same password for multiple websites. |
| 4 | Using online storage systems to exchange and keep personal or sensitive information. |
| 5 | Entering payment information on websites that have no clear security information/certification |
| 6 | Using free-to-access public Wi-Fi |
| 7 | Relying on a trusted friend or colleague to advise you on aspects of online-security. |
| 8 | Downloading free anti-virus software from an unknown source. |
| 9 | Disabling the anti-virus on my work computer so that I can download information from websites. |
| 10 | Bringing in my own USB to work in order to transfer data onto it. |
| 11* | Checking that software for your smartphone/tablet/laptop/PC is up-to-date. |
| 12 | Downloading digital media (music, films, games) from unlicensed sources |
| 13 | Sharing my current location on social media. |
| 14 | Accepting friend requests on social media because you recognise the photo. |
| 15 | Clicking on links contained in unsolicited emails from an unknown source. |
| 16 | Sending personal information to strangers over the Internet. |
| 17 | Clicking on links contained in an email from a trusted friend or work colleague. |
| 18* | Checking for updates to any anti-virus software you have installed. |
| 19 | Downloading data and material from websites on my work computer without checking its authenticity. |
| 20 | Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop) |

* Indicates reverse scored items.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

ATC-IB could range from 25–100. Cronbach's Alpha for the original 25-item scale was .744, and showed that three items had poor inter-item correlations (items 11, 12 and 24). The removal of these items increased Cronbach's Alpha to .80, indicating a high level of reliability. The full list of items for this scale is shown in Table 2.

### 2.2.5. Ethical considerations

This project was reviewed and approved in accordance with the operational procedures for De Montfort University's Faculty of Health and Life Sciences Research Ethics Committee (ref. 1605). Participants were informed of their right to

**Table 2.** Scale items for the Attitudes towards Cybersecurity and Cybercrime Questionnaire (ATC-IB).

| | Item |
|---|---|
| 1 | I think that management have the responsibility to ensure a company is protected from cybercrime |
| 2* | I am aware of my role in keeping the company protected from potential cybercriminals. |
| 3 | I believe everyone in the company has a role to play in protecting against threats from cybercriminals. |
| 4 | It is hard to know how I can help protect the organisation from cybercrime. |
| 5 | I don't have the right skills to be able to protect the organisation from cybercrime. |
| 6 | I do not feel that IT security is a priority within my organisation. |
| 7 | Computer systems provide all the protection a company needs. |
| 8 | I think that reporting cybercrime is a waste of time. |
| 9 | The Police lack the capacity to deal with cybercrime effectively. |
| 10 | I believe that cybercriminals are more advanced than the people who are supposed to be protecting us. |
| 11 | I think that information provided by the Government and Police on cybercrime is not relevant to businesses.^ |
| 12 | I feel that the Police are far too busy to deal with cybercrime.^ |
| 13 | I worry that if I report a cyberattack to the Police it might damage the reputation of the company |
| 14* | I think more could be done to communicate the risks from cybercrime to individuals in the organisation. |
| 15* | I am aware of the company's IT use policy and attempt to follow it. |
| 16 | I would not know how to report a cyberattack if one happened. |
| 17 | I don't think that reporting a cyberattack on the company is my responsibility. |
| 18 | I don't pay attention to company material about the threats from cybercrime. |
| 19* | I am confident that I would be able to spot the signs of a cyberattack. |
| 20* | I think the biggest threat for IT systems comes from people within the company. |
| 21* | I feel that any individual within the company are at risk of manipulation from confidence tricksters. |
| 22 | I think that cybercriminals only target a company when there is a substantial financial gain. |
| 23 | I believe only large companies are targeted by hackers and cybercriminals. |
| 24 | I feel that only companies that take payments using online systems are at risk of being victims of cybercrime.^ |
| 25 | I don't think I know who is responsible for protecting the company from cybercrime. |

^Indicates items that were omitted from the final scale due to poor inter-item correlation.
* Indicates items that were reversed scored.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

withdraw from the survey at any point, activated by clicking a 'withdraw now' option presented on each page. Clicking this option presented participants with a full debrief screen detailing the aims and objectives for the study and further contact details of the researcher. Participants indicated their informed consent by clicking on an option at the end of the information sheet detailing that they had read all the relevant information and were happy to continue.

### 2.2.6. Data collation

Of the 538 participants who completed the survey, a total of 23 were omitted from the final analysis due to incomplete information. The remaining dataset contained responses from 515 respondents.

For the RScB, two items were reverse scored (items 11 and 18). In the instance of the ATC-IB, 6 items were reversed scored (2, 14, 15, 19, 20 and 21). The OCS contained one reverse-score item (12). For each of these scales, a total score was calculated.

For the ABIS scale, adding the relevant items together and averaging the responses calculated the three subscales. For the first scale of attention, items 5, 8*, 9*, 12* and 20* were included. Motor impulsiveness includes items 2, 14, 17 and 18. Finally Non-planning impulsiveness included items 1*, 7*, 13* and 26*. All items indicated by an asterisk were reversed scored. As researchers such has (Coutlee et al., 2014) argued against the unidimensionality of impulsivity a total score was not calculated, but instead each scale was treated as a separate element.

## 3. Results

Table 3 provides the means and SDs for all measures alongside the correlations between the variables. Examinations of the distributions for each variable using histograms and P-P plots suggested that data could be treated as normal.

**Table 3.** Correlations, means and standard deviations for key variables.

| | Mean | SD | Imp Attention | Imp Motor | Imp Non-Planning | ATC-IB | OCS |
|---|---|---|---|---|---|---|---|
| Imp Attention | 2.07 | 0.52 | – | | | | |
| Imp Motor | 2.03 | 0.58 | .36** | – | | | |
| Imp Non-Planning | 2.33 | 0.61 | .60** | .14** | – | | |
| ATC-IB | 60.19 | 7.31 | -.24** | -.24** | -.11* | – | |
| OCS | 119.30 | 37.44 | .21** | .35** | .00 | -.40** | – |
| RScB | 27.72 | 14.81 | .15** | .30** | -.30 | -30** | .36** |

** $p < 0.01$ Level (2-tailed).

* $p < 0.5$ Level (2-tailed).


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

### 3.1. Internet addiction and attitudes towards cybersecurity on risky cybersecurity behaviours

A hierarchical regression was conducted to see if the two predictors of Internet addiction and attitudes towards cybersecurity predicted risky cybersecurity behaviour scores. Based on research by Griffiths (2010) and Stanton (2002), Internet addiction was entered in the first step, and attitudes towards cybersecurity entered in the second.

The Durbin-Watson statistic was 1.896, suggesting that independence of errors could be assumed, and values of tolerance and VIF suggested that multicollinearity was not a concern (VIF average = 1.19, tolerance average = .840). Collinearity diagnostics indicated no multicollinearity.

Model 1 presented a statistically significant fit to the data, ($F(1, 513) = 78.074$, $p < .001$, $R^2 = .132$, $R^2_{Adjusted} = .130$) explaining 13% of the variance in risky cybersecurity behaviours. Model 2 was also a good fit to the data, ($F(2, 512) = 49.279$, $p < .001$, $R^2 = .161$, $R^2_{Adjusted} = .158$) with the additional predictor explaining an additional 3% of variance.

As can be seen in Table 4, Internet Addiction and Attitudes towards Cybersecurity both presented as significant predictors towards risky cybersecurity behaviours.

### 3.2. Impulsivity and risky cybersecurity behaviours

A second regression was conducted in which all of the impulsivity subscales were entered simultaneously. The value of the Durbin-Watson statistic was 1.939, suggesting that independence of errors could be assumed, and values of tolerance and VIF suggested that multicollinearity was not a concern (VIF average = 1.49,

**Table 4.** Linear model for OCS and ATC-IB as predictors of Risky Cybersecurity Behaviours.

| | *B* | *SE B* | *β* | *p* |
|---|---|---|---|---|
| **Step 1** | | | | |
| *Constant* | 6.572 | 2.034 | | .001 |
| *OCS* | .144 | .016 | .363 | .000 |
| **Step 2** | | | | |
| *Constant* | 32.888 | 6.532 | | .000 |
| *OCS* | .144 | .017 | .289 | .000 |
| *ATC-IB* | -.379 | .089 | -.187 | .000 |

Note. $R^2 = .0.132$ for Step 1; $R^2 = .161$ for Step 2.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

tolerance average = .690). Collinearity diagnostics also indicated no multi-collinearity. The linear model for the regression is presented in Table 5.

The model presented a statistically significant fit to the data, ($F(3, 511) = 18.130$, $p < .001$, $R^2 = .096$, $R^2_{Adjusted} = .091$) explaining 9% of the variance in risky cybersecurity behaviours.

## 4. Discussion

The current study aimed to explore potential variables that could serve to predict a higher frequency for engaging in risky cybersecurity behaviours. The results present a preliminary step into exploring human factors within cybersecurity. There is the potential for certain predictors to provide a mechanism for identifying those who may be more susceptible to engage in cyber-related risky behaviours. Each of these will now be discussed in turn.

### 4.1. Attitudes towards cybersecurity and risky cybersecurity behaviours

One of key findings from the current research is that employee attitudes towards cybersecurity were negatively correlated to the frequency with which they engaged in risky cybersecurity behaviours. The capacity to instil good cybersecurity behaviour should be viewed as being of paramount importance for all organisations, irrespective of their size and complexity. However, it is apparent that from the responses to the attitude scale this is not the case, with pockets of individuals appearing to be disengaged or ill equipped to act appropriately. Some 98% of those questioned devolved responsibility of company cybersecurity to management, with a further 58% stating they did not know how they could protect the company from cybercrime. One analogue to this is found in Tischer et al. (2016), who noted that certain individuals appear to devolve aspects of their security to computer systems. In the context of the present study the concept of 'computer systems' may also extend to include other aspects of the work-based

**Table 5.** Linear model for ABIS Subscales as predictors of Risky Cybersecurity Behaviours.

| | *B* | *SE B* | *β* | *p* |
|---|---|---|---|---|
| *Constant* | 9.307 | 3.173 | | .004 |
| *Attention* | 3.727 | 1.598 | .130 | .020 |
| *Motor* | 6.642 | 1.154 | .261 | .000 |
| *Non-Planning* | -2.902 | 1.274 | -.120 | .023 |

Note. $R^2 = .0.096$.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

environment, including system administrators and management. It would appear that these are the people who individuals believe have a direct responsibility for prevention from cyberattacks. It would also appear that those individuals who are dismissive or are ignorant to the threats from poor cybersecurity are more likely to engage in risky cybersecurity behaviours. It is unclear if this is due to a complete disregard for information security or the belief that technology-based security measures will protect an individual from cybercrime, and provides a route for further empirical study. One of the key reasons for employing the use of an attitude scales in research of this nature is that, given the capacity for attitudes to change over time, it provides a good metric to examine if interventions have served to alter knowledge and perceptions (Shropshire et al., 2006).

## 4.2. Internet addiction and risky cybersecurity behaviours

The extent to which individuals engage in risky cybersecurity behaviours also appears to be closely linked to the level of problematic or addictive Internet use they exhibit. At the heart of behavioural addiction is the drive to engage in the addictive behaviour, which goes above all else and dominates the individual's thoughts, feelings and behaviours (Giffiths, 2010). This concept of 'salience' may be one potential element of the addictive complex that overrides a capacity to engage in good cybersecurity behaviours. Griffiths (2010) discussed the capacity for Internet addiction to lead to aspects of Internet abuse within the workplace, with the present study representing one of the first to link the potential impact on the cybersecurity of the organisation. In very early work of this nature, Stanton (2002) had suggested that there was the potential for a small proportion of employees who were addicted to the Internet to also abuse Internet access at work. In the context of the present study Internet addiction is not presented as a potential screening tool to isolate individuals in order for punitive action to be taken. Researchers such as Young and Case (2004) suggested that caution should be exercised when attempting to punish individuals who exhibit problematic Internet use in the workplace. By doing so, the employer could be creating even wider issues, and they advise support and the provision of potential routes to therapeutic interventions as a more effective approach.

## 4.3. Impulsivity and risky cybersecurity behaviours

The three subscales included in the ABIS all presented significant predictors for risky cybersecurity behaviours. Attentional and Motor impulsivity both presented as significant positive predictors for risky behaviours. Based on past research it is assumed that those with high levels of impulsiveness often act without reflection and pay little attention to the cost of their actions (Coutlee et al., 2014). This 'think before you act' behaviour may be a key mechanism that serves to override engagement in positive cybersecurity practices. Individuals may engage in risky


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

cybersecurity behaviours without fully establishing the cost of doing so, not only for them but also the company for whom they work.

The Non-Planning element of impulsivity was found to be a significant negative predictor for risky cybersecurity behaviours. This suggests that individuals who plan for short-term and long-term goals, in turn less likely to rush to complete activities, and in turn are not jeopardising cybersecurity as a result. These findings differ from previous research which noted negative correlations between the sub-scales of the BIS-11 and the SeBIS (Egelman and Peer, 2015a, b)). However qualitative differences in the content of the scales used could be one potential reason for the difference in results, and it suggested that further studies aim to clarify this. It is also noted that impulsivity accounted for just 9% of the overall variance in the data, suggesting that other factors could be contributing to the difference in risky behaviours.

## 4.4. Limitations for the present study

There are a number of limitations attached to this study, a key one being the reliance on self-reporting. Individuals who responded to the survey could have answered in an attempt to portray a 'perfect' set of cybersecurity behaviours rather than fully disclosing the true nature of their potential transgressions online. This in part would mean that the risky cybersecurity behaviours individuals were admitting to fails to fully tap into what they were actually doing on a day-to-day basis. The only viable mechanism available to counter this would be to implement work-based monitoring to record actual behaviours, which could in turn create more serious issues related to the ethics of such a process.

The notion of risk compensation (Wilde, 1998) also presents a potential confound in the context of the present study. The example often presented in the context of risk compensation is the use of seat belts in automobiles. The logic here is that drivers believe they are more protected by wearing a seat belt in contrast to not wearing one, and therefore will take more risks. This has a direct link to information security behaviours, particularly when the individual is in a place of work. Many working environments employ information technology infrastructures that are protected by a variety of technical countermeasures designed to prevent potential breaches. As the individual believes they are more protected in the workplace they may be inclined to take more risks, circumvent accepted protocols and engage in poorer information security behaviours. This proposition is couched very much in a tentative way, and there is need to explore this in more detail through further research.

It is also noted that the use of the term 'Internet addiction' can present its own set of issues, and in light of commentary presented by other researchers (Griffiths, 1998; Kuss et al., 2014) an awareness of such issues should be accepted in the

 http://dx.doi.org/10.1016/j.heliyon.2017.e00346

interpretation of these findings. The actual evidence of pure Internet addiction is limited, with only a small number of cases actually being reported (Kuss et al., 2014). From this perspective further research is required to explore how technology addiction as a whole serves to impact potentially risky cybersecurity behaviours.

## 5. Conclusion

As the fight against susceptibility to cybercrime and the prevention of digital attacks within businesses moves an emphasis away from technology towards human factors, research of this nature becomes more and more important. The present research highlights how aspects of personality, problematic Internet use and employee attitudes can impact on the potential to engage in effective information security behaviours. As a more systematic model of how individuals are choosing to engage (or not) in good cybersecurity practices is developed, there is the potential to create clearer communications packages or strategies to proliferate these further. Some work has already been conducted in this area, with research from Bada et al. (2014) noting that in order to be effective, key design elements have to be adhered to. For instance the researchers noted that information security education has to go beyond just providing information to users. In order to circumvent this, it is suggested that information has to be targeted, has to be actionable, relevant, and there must be the provision of feedback so that individuals can assess how well they are performing (Bada et al., 2014). Such measures also present the possibility for identifying those individuals who present a higher risk to an organisation in terms of a lack of adherence to good cybersecurity practices, allowing these individuals to be educated or trained further rather than punished.

## Declarations

### Author contribution statement

Lee Hadlington: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

### Funding statement

This work was supported by East Midlands Police Academic Collaboration (J014) and the College of Policing and the Higher Education Funding Council for England (HEFCE).

### Competing interest statement

The authors declare no conflict of interest.


http://dx.doi.org/10.1016/j.heliyon.2017.e00346

## Additional information

No additional information is available for this paper.

## References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2016. Gender difference and employees' cybersecurity behaviors. Comput. Human Behav. 69, 437–443.

Bada, M., Sass, A.M., Nurse, J.R.C., 2014. Cyber Security Awareness Campaigns Why do they fail to change behaviour? Global Cyber Security Capacity Centre: Draft Working Paper, 118–131.

Chen, J.V., Chen, C.C., Yang, H.-H., 2008. An empirical evaluation of key factors contributing to internet abuse in the workplace. Ind. Manage. Data Syst. 108 (1), 87–106.

Coutlee, C.G., Politzer, C.S., Hoyle, R.H., Huettel, S., 2014. An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version 11. Arch. Sci. Psychol. 2, 1–12.

Davis, R.A., Flett, G.L., Besser, A., 2002. Validation of a new scale for measuring problematic Internet use: Implications for pre-employment screening. Cyberpsychol. Behav. 5 (4), 331–345.

Egelman, S., Peer, E., 2015a. Predicting Privacy and Security Attitudes. Computers and Society: The Newletter of ACM SIGCAS 45 (1), 22–28.

Egelman, S., Peer, E., 2015b. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS) (CHI' 15). Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems 1, 2873–2882.

Giffiths, M., 2010. Internet abuse and internet addiction in the workplace 22 (7), 463–472.

Greenfield, D.N., Davis, R.A., 2002. Lost in cyberspace: the web at work. Cyberpsychol. Behav. 5 (4), 347–353.

Griffiths, M., 1998. Internet addiction: Does it really exist? In: Gackenbach, J. (Ed.), Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications. Academic Press, San Deigo, CA, pp. 61–75. http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=1998-06638-003&site=ehost-live.

Griffiths, M., 2000. Internet addiction – time to be taken seriously? Addict. Res. 8 (5), 413.

Griffiths, M., 2010. Internet abuse and internet addiction in the workplace. Journal of Workplace Learning 22 (7), 463–472.

 http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Herath, T., Rao, H.R., 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47 (2), 154–165.

Herath, T., Rao, H.R., 2009b. Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. Eur. J. Inf. Syst. 18 (2), 106–125.

HM Government, 2015. Information Security Breaches Survey. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

HMSO, 2010. A Strong Britain in an Age of Uncertainty: The National Security Strategy. http://www.official-documents.gov.uk/.

John, O.P., Srivastava, S., 1999. Big Five Inventory (Bfi). Handbook of Personality: Theory and Research 2, 102–138.

Karaiskos, D., Tzavellas, E., Balta, G., Paparrigopoulos, T., 2010. Social network addiction: A new clinical disorder? Eur. Psychiatry 25 (1), 855–856.

Kuss, D.J., Griffiths, M.D., Karila, L., Billieux, J., 2014. Internet Addiction: A Systematic Review of Epidemiological Research for the Last Decade. Curr. Pharm. Des. 1 (4), 397–413.

Kuss, D.J., Louws, J., Wiers, R.W., 2012. Online Gaming Addiction? Motives Predict Addictive Play Behavior in Massively Multiplayer Online Role-Playing Games. Cyberpsychol. Behav. Soc. Netw. 15 (9), 480–485.

LaBrie, J., Collier, A., Palmer, A., 2010. Cybercrime Report: The Human Impact. .

Marulanda-Carter, L., Jackson, T.W., 2012. Effects of e-mail addiction and interruptions on employees. Journal of Systems and Information Technology 14 (1), 82–94.

McBride, M., Carter, L., Warkentin, M., 2012. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International–Institute of Homeland Security Solutions, North Carolina.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M., 2016. Individual differences and Information Security Awareness. Comput. Human Behav. 69, 151–156.

McCoul, M.D., Haslam, N., 2001. Predicting high risk sexual behaviour in heterosexual and homosexual men: the roles of impulsivity and sensation seeking. Pers. Individ. Dif. 31 (8), 1303–1310.

 http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Ng, B.D., Wiemer-Hastings, P., 2005. Addiction to the internet and online gaming. Cyberpsychol. Behav. 8 (2), 110–113.

Panko, R., 2010. Corporate Computer and Network Security, second ed. Prentice Hall, Upper Saddle River, NJ.

Pee, L.G., Woon, I.M.Y., Kankanhalli, A., 2008. Explaining non-work-related computing in the workplace: A comparison of alternative models. Inform. Manage. 45, 120–130.

Rosen, L.D., 2010. Rewired: Understanding the iGeneration and the way they learn. Macmillan, New York: Palgrave.

Shropshire, J., Warkentin, M., Johnston, A.C., Schmidt, M.B., 2006. Personality and IT security: An application of the five-factor model. Americas Conference on Information Systems (AMCIS), 3443–3449.

Shropshire, J., Warkentin, M., Sharma, S., 2015. Personality, attitudes: and intentions: Predicting initial adoption of information security behavior. Comput. Sec. 49, 177–191.

Stanton, J., 2002. Company Profile of the Frequent Internet User. Communications of the ACM 45 (1), 55–59.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., Bailey, M., 2016. Users Really Do Plug in USB Drives They Find. IEEE Symposium on Security and Privacy, 1–14.

Uebelacker, S., Quiel, S., 2014. The Social Engineering Personality Framework. Workshop on Socio-Technical Aspects in Security and Trust, 24–30.

Weatherbee, T.G., 2010. Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. Hum. Resource Manage. R. 20 (1), 35–44.

Welk, A.K., Hong, K.W., Zielinska, O.A., Tembe, R., Murphy-Hill, E., Mayhorn, C.B., 2015. Will the Phisher-Men Reel You In? International Journal of Cyber Behavior Psychology and Learning 5 (4), 1–17.

Wilde, G.J., 1998. Risk homeostasis theory: an overview. Injury Prevention 4 (2), 89–91.

Young, K.S., 1998. Internet addiction: The emergence of a new clinical disorder. Cyberpsychol. Behav. 1 (3), 237–244.

Young, K.S., Case, C.J., 2004. Internet abuse in the workplace: new trends in risk management. Cyberpsychol. Behav. 7 (1), 105–111.

 http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Zuckerman, M., Kuhlman, D.M., 2000. Personality and risk-taking: common biosocial factors. J. Personal. 68 (6), 999.

 http://dx.doi.org/10.1016/j.heliyon.2017.e00346