Article

Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors

Lee Hadlington* and Sally Chivers**

Abstract The present article aimed to explore if susceptibility to cybercrime can be linked to information security awareness and personality factors. A total of 1,054 participants aged between 18 and 84 years took part in an online survey consisting of a recently developed segmentation analysis tool designed to explore an individual's susceptibility to cybercrime. Alongside this, two other scales measuring information security awareness and the personality trait of impulsivity were also included. In total, 60% of the population surveyed presented as being in the higher risk categories for susceptibility to cybercrime. Furthermore, individuals in the higher risk categories for susceptibility to cybercrime also presented poorer information security awareness, as well as having higher levels of trait impulsivity. It was also noted that certain demographic factors also linked to susceptibility to cybercrime, including age and current employment status, with the unemployed and student populations being less well represented in lower risk categories. This work is seen as being critical while designing effective intervention strategies that are designed to target specific at-risk populations, as well as presenting a key tool that could be widely used by organizations to examine risk within their own specific populations.

Introduction

In 2015 the Home Office National Security Strategy confirmed the threat from cyber-related incidents as a Tier One risk to UK interests (HM Government, 2016). The strategy presents a key means to mitigate the evolving UK cyberthreat, as well as arming citizens with the capacity to defend themselves. The report cited poor cyber hygiene, poor security compliance, and a lack of training and skills as issues directly linked to human behaviour which ultimately affect cyber security. Significantly, the report noted that:

> Cyber attacks are not necessarily sophisticated or inevitable and are often the result of exploited—but easily rectifiable and, often preventable—vulnerabilities (HM Government, 2016, p. 22)

The report also suggested that it is the continuing vulnerability of the victim, rather than the

*Psychology Division, De Montfort University, Leicester, UK. E-mail: lhadlington@dmu.ac.uk
**Division of Community and Criminal Justice, De Montfort University, Leicester, UK

Policing, pp. 1–14
doi:10.1093/police/pay027
© The Author(s) 2018. Published by Oxford University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

complexity of the attack, that presents the key to the success of a cyberattack.

The government report (2016) is aligned to a growing realization by those working in the area of information security that human behavioural factors hold the key to understanding (and therefore mitigating) the continued susceptibility to cybercrime (Anwar *et al.*, 2017; Furnell and Clarke, 2012). To date, the use of security protocols and technical interventions have failed to protect individuals from cyberattacks (Herath and Rao, 2009). One of the reasons for the failure of such technological interventions is that individuals either fail to follow advisory preventative protocols, circumvent them, or engage in behaviours that put them at increased risk (Hadlington, 2017; Hadlington and Parsons, 2017). It is from this perspective that our study is presented, adding to the growing body of research exploring critical human factors in the context of cybercrime.

Segmentation analysis for susceptibility to cybercrime

A report by the Home Office (HO RICU, 2015) outlined the potential to segment the general population into key categories according to their level of susceptibility to cybercrime. The report presents eight categories (or segments) into which individuals can be classified based on their responses to a series of questions related to crime awareness and level of trust (HO RICU, 2015). The segments and their associated attributes are summarized below in Table 1. Exploring the findings from the original piece of research from the Home Office (HO), two key segments present as being the most digitally savvy and protected in the online digital environment; A: Already Protected and C3: Relatively Savvy. The remaining 66% of the population studied are presented as being those potentially at higher risk of becoming susceptible to cybercrime.

Having the capacity to understand the susceptibility of individuals to cybercrime is useful for a number of reasons. Primarily, it highlights the potential risk that exists in the current population at any given time, therefore offering a way to exploit crime prevention strategies for the most effective outcomes. Such preventative measures are able to target particular 'at-risk' groups rather than attempting to use a 'one-size-fits-all' approach. However, a degree of caution is suggested when using segmentation analysis, as it is only useful when isolating groups based on their proposed susceptibility to cybercrime. The HO analysis only presented very broad details of the types of behaviours that could potentially lead to potential susceptibility to cybercrime, an issue that the current research aims to address. Additionally, the original HO RICU (2015) segmentation failed to provide a objective measure of trait impulsivity, which is proposed as a key personality factor in terms of risky cybersecurity behaviours (Hadlington, 2017). In order to overcome this issue, the present study employs the use of two further measures, one related to knowledge, attitudes, and behaviours in the context of information security, the other measuring trait impulsivity.

Assessing information security

A number of researchers have attempted to measure the extent to which individuals adhere to information security advice. These measures have focused predominantly on assessing the information security awareness of individuals in a work-based environment; in such an environment there is generally a clear set of rules governing the use of work-based computer technology. Measurement scales have also focused on narrow aspects of information security, such as the use of password protection (Stanton *et al.*, 2005), the use of mobile device protection (Mylonas *et al.*, 2013), or on security features related to specific programmes (Furnell *et al.*, 2006).

One of the most recently developed scales exploring the information security awareness of individuals

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

Table 1: Segmentation Classifications taken from the HO RICU (2015) Report

Segment	Label	Percenatge population	Personality traits	Behaviours	Who are they?
A	Already Protected	13	Confident, cautious, considered; Do not make snap decisions; Not easily swayed + not afraid to say 'no'	Strong protection (on and offline)—marginally less likely to use social media regularly	Couples living with children Over 50s not living with children
B	Digitally Vulnerable	9	Suspicious of strangers on the street; not comfortable with technology (lower use of Internet); Do not worry about becoming a victim of cybercrime	Good offline protection; do not engage with cold callers/ strangers off the street; ensure financial documents are destroyed + check bank details; limited technical knowledge about how to browse Internet safely—do not use the Internet as much as general population	Aged 50–64 Lower income pensioners, unlikely to have formal qualifications
C1	Trusting	15	Too much trusting of others and easily swayed; a low propensity to challenge other	Moderate levels of protection to prevent off and online financial crimes; more likely to have been affected by scams involving upfront payments and sharing personal information	Young adults—typically 16–29; students, typically do not have children
C2	Unconcerned and Somewhat Protected	18	A tendency to act in a rash or 'spur of the moment' manner	Moderate levels of protective behaviours both on- and offline; Higher than average at engaging people in the street; more likely to be a victim of upfront payment scams, tricked into sharing data online	Most likely men aged 16–34; students and young professionals; typically do not have children
C3	Relatively Savvy	20	Relatively 'sensible' group; more likely to challenge others and are not easily swayed	Make a reasonable effort to protect themselves; moderate levels of offline and financial protection; well protected online	Very well educated and in full-time employment More likely to have teenage children; less likely to live on their own
D1	Unsuspecting and Unprotected	8	Highly malleable and trusting of others; Tend to go along with what others want and unlikely to challenge; Do not feel confident or prepared for every eventuality.	Very low levels of online, offline and financial protection	Young people still in school and university; generally well educated
D2	Unconcerned and Unprotected	9	Willing to take risks and choose to ignore consequences; Not overly trusting or easily swayed by others	Very low levels of protection both on and offline; particularly bad at password protection	Tend to be students and tend to typically live with parents; tend not to have children
E	Unaware	7	Believe in fate; Low propensity to challenge others; Do not worry about online crime (less likely to be online)	Moderate levels of protection for offline and financial; Low level of protection for online crimes	Female; Live with partner + child; Less educated

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

within a work-based context is the Human Aspects of Information Security Questionnaire (HAIS-Q; Parsons *et al.*, 2017). The HAIS-Q has been engaged in a variety of research projects, as well as being tested across a wide number of populations, hence establishing a robust reliability (see Parsons *et al.*, 2017). The HAIS-Q research questionnaire identified that information security awareness differs significantly across age ranges, and that increased awareness is positively correlated with personality factors including agreeableness (warmth), conscientiousness, and openness to experience. Conversely, negative correlations are highlighted for risk-taking and reduced information security awareness (McCormac *et al.*, 2017). Given the reliability of the HAIS-Q, as well as its capacity to divide information security awareness into a number of consistent factors, it was adopted as the framework for the Information Security Awareness scale used in the current study.

Researchers have also examined the way in which broader personality factors can influence the uptake of information security advice. For example, Egelman and Peer (2015) noted that the trait of impulsivity was negatively associated with good cybersecurity behaviours. 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 also demonstrated that higher levels of impulsivity are associated with an increased frequency of individuals engaging in risky online behaviours: this could place them at risk of being a victim of cybercrime (Hadlington, 2017). In the context of individual susceptibility to cybercrime, the measure of impulsivity appears to be a relevant personality factor to compare with the HO segmented population data. Although the original segmentation analysis mentions aspects of impulsivity, these elements are based on a series of behavioural and attitudinal questions, rather than being specifically measured through a psychologically validated scale. It is therefore suggested that further research is needed to support the connection between levels of impulsivity and susceptibility to cybercrime. Our study seeks to fill this gap.

Aims and objectives

The segmentation analysis framework provided by the HO RICU (2015) report presents a useful tool for examining the susceptibility of individuals to cybercrime. However, there are some gaps in its coverage, and although it highlights susceptibility, it fails to fully explore the potential reasons for susceptibility. It is from this perspective that the current study aims to explore how the segmented population maps onto a measure of information security awareness. In this way, it is proposed that the shortcomings identified in each of the HO population segments can be more clearly addressed. Alongside this, an additional measure of impulsivity was used to assess how these human factors can be linked to the susceptibility to suffer cybercrime. A secondary aim for the current research is to test the feasibility of developing the HO segmentation analysis into an online survey, omitting the need for an individual researcher to contact and question the respondent, as was the case in the original HO study. An online survey would give the opportunity to contact individuals via email and local messaging services to undertake the survey, broadening the potential reach of inclusion. This segmented population can be used to target training, communication, and interventions to enhance public and organizational awareness about cybercrime. Training initiatives, awareness campaigns, media communications and interventions all form part of police crime reduction and detection strategies. This segmented population approach has the capacity to increase the effectiveness of those strategies.

Methodology

Participants

A total of 1,054 participants aged between 18 and 84 years (mean = 41.20; SD = 15.98) were recruited

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

Table 2: Demographic data according to East Midlands Force Region

	Derbyshire	Nottinghamshire	Leicestershire and Rutland	Lincolnshire	Northamptonshire	Total
Gender						
Male	60	138	92	65	47	402
Female	110	191	117	105	74	597
Employment status						
Employed	112	208	125	104	78	627
Unemployed	27	56	38	26	18	165
Retired	19	36	27	29	18	129
Student	12	29	19	11	7	78
Age range (years)						
18–21	22	42	21	24	9	118
22–30	26	58	47	35	25	191
31–40	41	76	40	30	27	214
41–50	29	58	40	26	21	174
51–60	28	55	30	24	19	156
61+	24	40	31	31	20	146

from the East Midlands via Qualtrics Participant Panels to take part in an online survey. After the data was checked for incomplete responses or anomalies (e.g. participants choosing the same response for all items), a total of 999 participants' data were used in the final analysis. In this final sample there were a total of 402 males and 597 females, with an age range of 18–66 years (mean = 41.20, SD = 15.98). Full details of the demographics for the sample are included in Table 2.

Materials

Segmentation questionnaire

The Home Office Segmentation questionnaire consists of both attitudinal and behavioural components. It provides 26 questions, with participants responding on an 11-point Likert scale (0 = strongly disagree, 10 = strongly agree). Sample items from the scale include those that ask about awareness of Serious Organized Crime (e.g. Where people are tricked into sharing personal information or data following telephone or face-to-face conversations or where people have their personal information or data stolen, or attitudinal statements, e.g. 'Sometimes one needs to bend the rules to get ahead' or 'I prefer to agree with people in order to avoid confrontation'). The questionnaire is organized into a hierarchical tree structure, where individuals answer a minimum of three questions and a maximum of eight questions depending on responses. At the end of the questionnaire individuals are identified as belonging to a particular segment, outlining an individual's susceptibility to cybercrime. Full details of the structure of the questionnaire are available in the technical report (available from RICU@homeoffice.x.gsi.gov.uk).

The short human aspects in information security questionnaire

The original HAIS-Q developed by Parsons *et al.* (2014, 2017) was specifically designed to be used in a work-based business context where individuals are governed by a set of formal or informal information security rules. The HAIS-Q presents a unique structure insofar as it assesses information security awareness across three core elements; knowledge, attitude, and behaviour. The HAIS-Q also examines information security awareness across seven focus areas, including password management, email use, Internet use, social networking, incident reporting, mobile computing, and information handling

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

(Parsons *et al.*, 2014). A higher score on the HAIS-Q is indicative of a more positive engagement in aspects of information security.

The original HAIS-Q includes 63 individual questions, which could lead to a state of response fatigue in participants (see Parsons *et al.* (2017) for a full list of items). In order to counter fatigue when deploying the assessment tool in the general population, a modified, shortened version of the HAIS-Q (S-HAIS-Q) was developed for our study. The development of the scale aimed to retain the original structure in relation to knowledge, attitude, and behaviour across core information security areas. The S-HAIS-Q contained a total of 39 items, covering the core areas of password management, email use, website use, social media use, and the reporting of incidents. The list of items and the scoring profile for the S-HAIS-Q are included in Table 3. The scale showed good internal reliability, with a Cronbach's α of 0.921.

Abbreviated impulsiveness scale

A shortened 13-item impulsivity scale presented by Coutlee *et al.* (2014) was used to counter the potential for participant response fatigue. The abbreviated impulsiveness scale (ABIS) consists of three sub-scales, namely Attention, Motor, and Non-planning, with items being scored on a scale of 1 (Never/Rarely) to 4 (Almost Always/Always). Possible scores range from 13 to 52, where a lower score is indicative of an individual who is less impulsive and takes more time focus on individual tasks. The aspect of Non-planning impulsivity reflects the tendency for an individual to think before he or she acts, or the tendency to lack preparation in his or her actions. This also includes a lack of planning for both short-term concrete aims (e.g. trips or tasks), as well as longer term abstract aims (e.g. job security or future plans) (Coutlee *et al.*, 2014). Motor impulsivity is reflected in spontaneous, reactive, and uninhibited actions, and Attentional impulsivity is linked to inconsistencies in controlling thoughts and the capacity to focus attention. Coutlee *et al.* (2014) reported Cronbach's α of 0.80, 0.82, and 0.71, respectively, for each of these sub-scales.

Results

The following section reports the key trends within the data according to the key demographics and variables collected.

Key demographics and segmentation

In this section, the data related to specific demographic variables and the outputted segments are presented. Figure 1 presents the breakdown of our total sample according to HO RICU (2015) report. The primary segment represented within the data is C2: Unconcerned and Somewhat Protected: this accounted for 31% of the total population. This was closely followed by the C3: Relatively Savvy group, which accounted for 27% of the total population. The A: Already Protected segment accounted for just 13% of the total population. Exploring the data as a whole, and assuming that segments A and C3 represent individuals with the lowest susceptibility to cybercrime, a total of 60% of our sampled population demonstrate a high susceptibility to being a victim of cybercrime (this comprises segments B, C1, C2, D1, D2, and E).

The breakdown of segmentation by age range is presented in Fig. 2. It is noted that that there are some distinct differences in age range between the segments. The higher at-risk segments are a feature of the under 40 age groups. For example, 66% of those aged between 18 and 40 years fell into the D1: Unsuspecting and Unprotected segment; 60% fell into the E: Unaware segment; 61% were classified as Digitally Vulnerable. In contrast, 70% of those in the 41 and above age bracket were classified as A: Already protected. Such findings present a clear contrast to the often-presented view that it is the older generation that is potentially more vulnerable to cybercrime (Oksanen and Keipi, 2013).

Figure 3 presents a regional breakdown of the segmentation across the five police service

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

Table 3: S-HAIS-Q items according to focus area and sub-category

	Knowledge	Attitude	Behaviour
Focus area: Password management			
Sharing passwords	It is okay to share my passwords with friends.[a]	It is a bad idea to share my passwords, even if a friend asks for it.	I share my passwords with friends.[a]
Using a strong password	Strong passwords should have a mix of letters, numbers, and symbols.	It is safe to have a password with just letters.[a]	I use passwords with letters, numbers, and symbols.
Focus area: Email use			
Clicking on links in emails from strangers	Clicking on links in emails from strangers could have serious consequences.	Nothing bad can happen if I click on a link in an email from a stranger.[a]	If an email from a stranger looks interesting, I would click on a link within it.[a]
Opening attachments in emails from strangers	It is not okay to open email attachments from people I do not know.	It is risky to open an email attachment from strangers.	I do not open email attachments from strangers.
Focus area: Internet use			
Accessing dubious websites	I know there are some websites that I should not access.	Just because I can access a website, does not mean that it is safe.	When online, I visit any website that I want to.[a]
Entering information online	It is okay to enter personal information on any website I visit.[a]	It does not matter what information I put on a website.[a]	I try to check the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I should always use privacy settings on my social media accounts.	It is a good idea to use social media privacy settings.	I do not use social media privacy settings.[a]
Considering consequences	I cannot get in trouble for something I post on social media.[a]	It does not matter if I post things on social media that I would not say in public.[a]	I do not post on social media without thinking about what might happen.
Friending on SNS	It is not okay to accept someone on social media just because I like their photo.	Nothing bad will happen if I accept friend requests from strangers on social media.[a]	I accept friend requests on social media based on just a photo.[a]
Focus area: Mobile devices			
Malware and Software updates	Computer viruses cannot really affect a smartphone or tablet.[a]	I do not worry about viruses on my smartphone as they only affect computers.[a]	I install software updates for my smartphone or tablet as soon as they are available.
Mobile safety	A password or PIN should be used to lock my smartphone or tablet.	I do not need to lock my smartphone as it is with me most of the time.[a]	I use a password or PIN to lock my smartphone or tablet.
Free-access Wi-Fi	It is risky to use free-to-access Wi-Fi to send personal details.	It is not risky to use free-to-access Wi-Fi to send personal details.[a]	I use free-to-access Wi-Fi for anything I need to do online.[a]
Focus area: Incident reporting			
Reporting suspicious behaviour	If something happens online that makes me feel bad, I should report it to someone (e.g. Police, Website Provider).	If I ignore something that makes me feel bad online, nothing bad can happen.[a]	If something happened online that made me feel bad, I would tell someone (e.g. Police, Website Provider).

Note: Participants are instructed to respond to each item on a five-point scale from 'Strongly Disagree' to 'Strongly Agree'.
aReverse scoring was used on this item.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

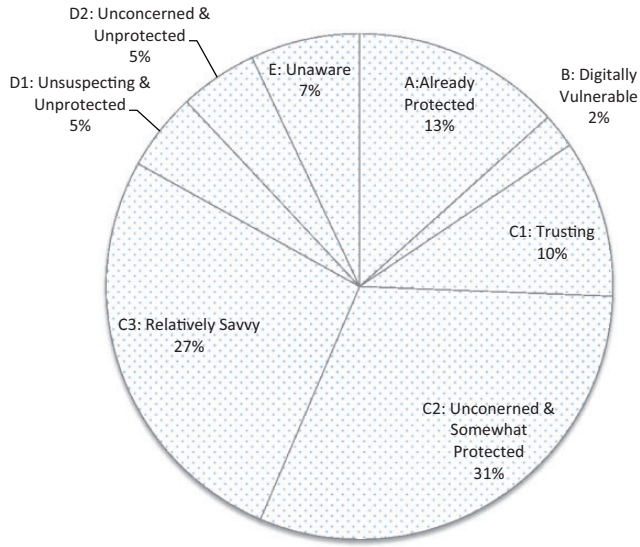

Figure 1: Segmented susceptibility to cybercrime in sample population (percentage of total population).

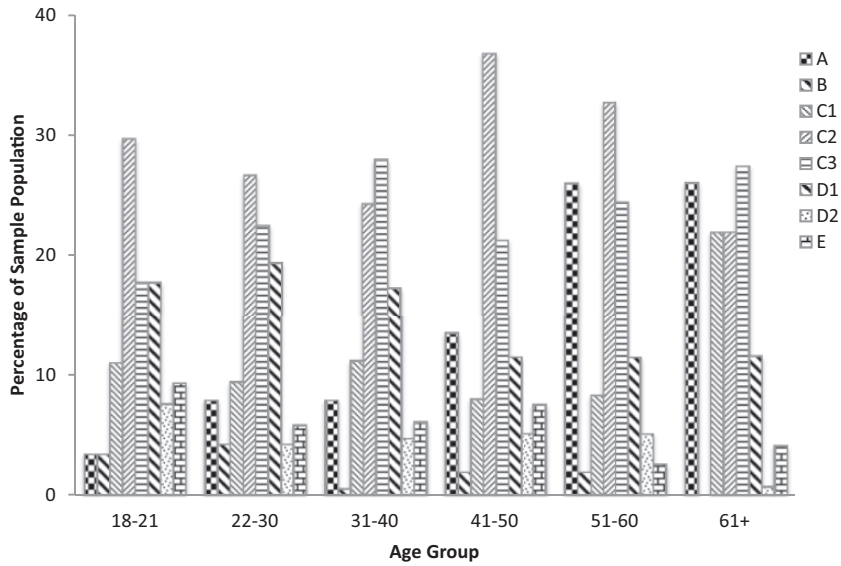

Figure 2: Segmentation by age group.

geographies. Notionally, the advantage of this information is the capacity to map this data onto crime figures produced by national bodies such as Action Fraud. Equally, when determining priorities for local targeted messaging systems, data such as this allow messages to be directed at high-risk groups. Nottinghamshire and Leicestershire and Rutland are the police service geographies with the highest number of individuals classified as A: Already Protected. Derbyshire has the lowest number in this category. Across all police service geographies, the C2: Unconcerned and Somewhat Protected segment features quite widely, together with the C3: Already Savvy segment.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

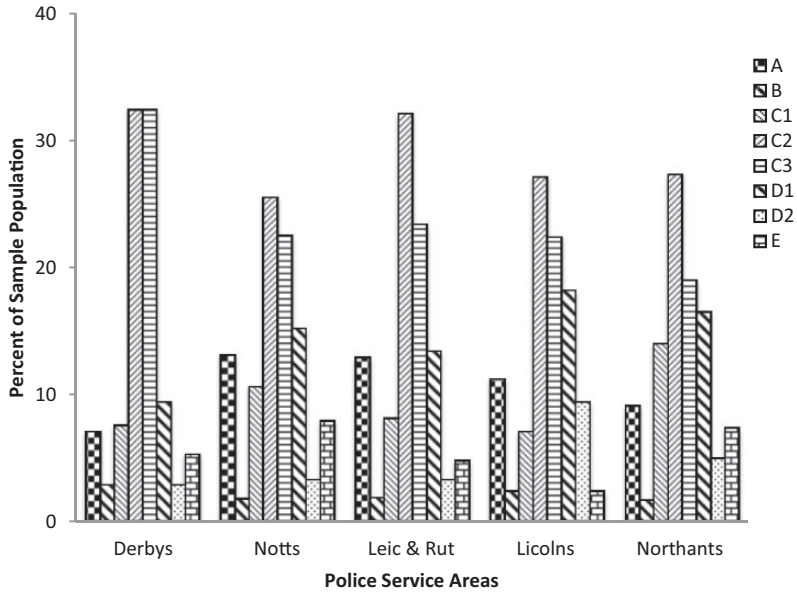

Figure 3: Segmentation by police service area.

When segmented according to employment status the data highlights another trend associated with the at-risk groups (see Fig. 4). Those in the A: Already Protected category are poorly represented in the employed and student populations compared with the unemployed and retired populations in the study. This finding is supported by findings from previous research which suggested undergraduate students in particular are susceptible to cybercrime due to a variety of key factors (Bidgoli *et al.*, 2016). Students were also more likely to fall into the C1: Trusting and C2: Unconcerned and Somewhat protected categories, but comprised the lowest number of individuals in the C3: Relatively Savvy category.

Information security measures and segmentation

In this section the results of the segmentation analysis are compared with data from the S-HAIS-Q measure of information security awareness. The data for the focus areas of the S-HAIS-Q according to segmentation are presented below in Fig. 5.

A key feature of these data is that the scores on the focus areas of the S-HAIS-Q map well onto suggested features of the segmentations. In this instance, a higher score on each of the scales indicates a higher level of adherence to accepted cybersecurity principles in each of the given areas. As noted, the A: Already Protected segment scores the highest on each of the core areas in comparison with the others, indicating higher levels of adherence and knowledge. This is closely followed by the C3: Relatively Savvy segment, which also shows consistently higher scores in each of the core areas. Conversely, the B: Digitally Vulnerable segment and the E: Unaware segment consistently fall below the other segmentations in terms of their adherence to accepted cybersecurity protocols on all of the core areas for the S-HAIS-Q.

Figure 6 highlights the differences in the three sub-scales of the S-HAIS-Q according to the categories of Knowledge, Attitude, and Behaviours of individuals. A higher score on the S-HAIS-Q is indicative of a better general awareness related to aspects of information security. The results map well onto the individual segments, showing that higher

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

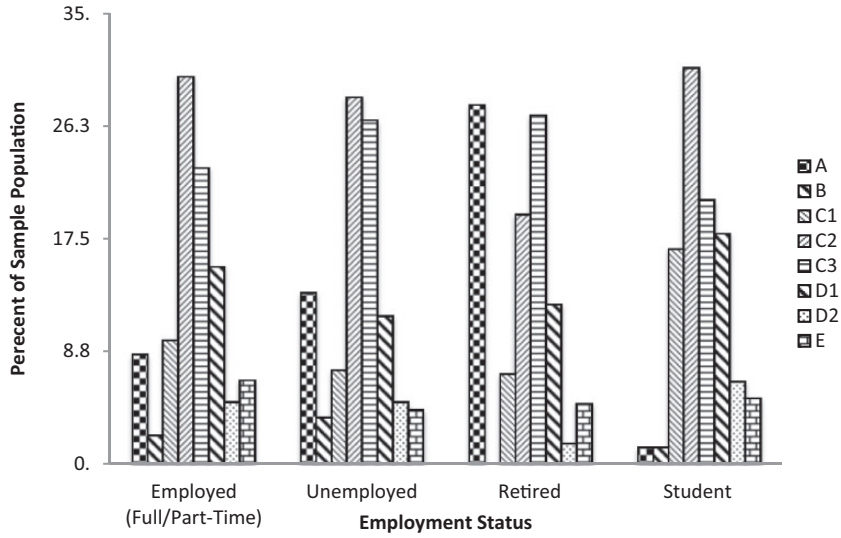

Figure 4: Segmentation by employment status.

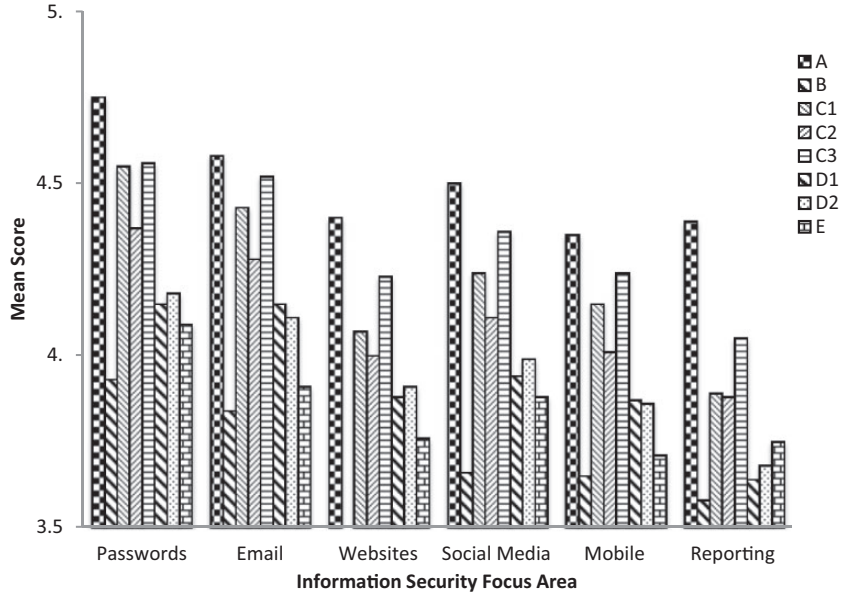

Figure 5: Information security focus area by segmentation.

scores on the three sub-scales are associated with lower levels of cybercrime susceptibility. For example, individuals in the A: Already Protected segments scored higher in all three measures in comparison with individuals in the other segments. In contrast, the individuals in the B: Digitally Vulnerable segment scored much lower on each of the three scales.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

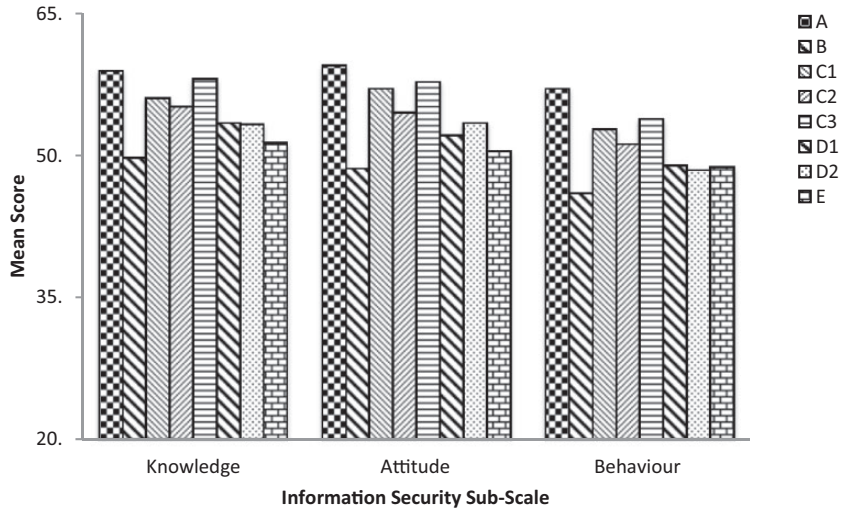

Figure 6: Knowledge, attitude, and behaviour in relation to online security by segmentation.

Psychometric measures according to segmentation

In terms of the data from the impulsivity measures, there appears to be a general tendency to support the original assumptions presented in the original HO RICU (2015) report (See Figure 7). The original report suggested that those individuals who have higher levels of impulsivity, thus lacking the capacity to 'think things over', take more risks online. In the context of the present study, a lower score for the impulsivity scales is indicative of a capacity to resist the urge to act on impulse and take time to think things over. Data reveal that those in the A: Already Protected segment scored lower on aspects of both attentional impulsivity and motor impulsivity in comparison with all other segments. Conversely, the B: Digitally Vulnerable segment scored the highest on all three measures for impulsivity.

Discussion

The findings from the current research highlight some critical observations about the susceptibility of individuals to cybercrime. Overall, the findings demonstrate that police service geographies figures are reflective of national trends taken from the HO RICU (2015) report, with 60% of those in the sample presenting a higher level of susceptibility to cybercrime. By implementing the use of two further measures that examined the information security behaviours of the participants and the trait of impulsivity, more detail is added to the generic segmentation presented by the HO RICU (2015) report. The finer details of the results will be considered in order to explore how they can assist police services in the targeting of crime prevention measures.

Segmentation and information security

By exploring the key findings that pair the segmentation analysis with the measure of information security awareness, it is clear that there is some consistency between the two measures. First, those segments that have the lowest level of susceptibility to cybercrime (A: Already Protected; C3: Relatively Savvy) demonstrated higher (positive) scores across all three key sub-areas of knowledge, attitude, and behaviour relating to information security. Interestingly, those individuals in the C1: Trusting segment demonstrated scores that were (positively) higher than the remaining segments,

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

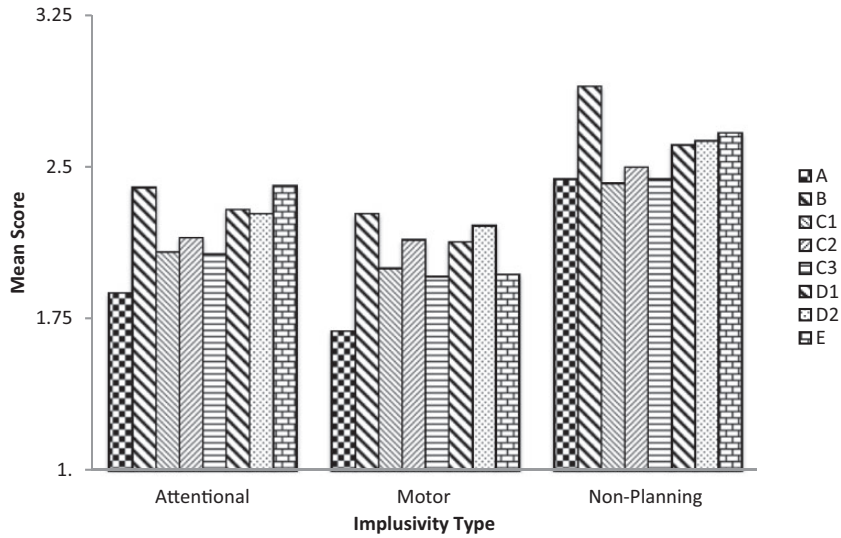

Figure 7: Impulsivity type by segmentation.

suggesting that their susceptibility to cybercrime comes from a facet not directly explored on the information security questionnaire. The B: Digitally Vulnerable segment was the group with the lowest scores across each of the information security questionnaire sub-scales. This is a critical finding, and suggests that the potential underlying factor for susceptibility of this group to cybercrime is a limited understanding of information security practices. It is clear that key messages related to cyber-related crime have so far produced little demonstrable effect on members of this group. For this reason further research is suggested in this area.

The A: Already Protected and C3: Relatively Savvy segmentations presented higher scores across the seven focus areas for cyber security. As might be expected, the A: Already Protected group showed particularly good information security in relation to password protection, the use of email, and the use of social media. However, all groups scored consistently lower on the core areas related to website use, suggesting that this area could also be the subject of enhanced crime prevention guidance. D1, D2, and E segmentations all scored lower on the aspect of reporting in the information security questionnaire; police targeted education and awareness messages have the potential to assist in these populations too.

Adding an information security awareness measurement to the segmentation analysis demonstrates that susceptibility to cybercrime can, in part, be linked to a weaker information security awareness position. A further benefit of using a scale such as the S-HAIS-Q is that it presents the opportunity to assess key aspects of online security in which segmented populations are prone to weakness. This is turn could be turned into a target tool designed to present communication messages in such weaker areas, hence reducing redundant messages.

Susceptibility to cybercrime and age

One of the most striking trends in the data from the present study is the difference between age groups and the susceptibility to cybercrime. There is an assumption that those in the 'digital native' (Prensky, 2001) generation, or those that have never experienced a world without the Internet, are best able to deal with the constant threat from cybercrime. This is contrasted with the view that those in the 'digital immigrant' population, who have risen to technology awareness later, are more vulnerable as they have less technical knowledge.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

The present data shifted this perception, demonstrating that it is the younger population who are most at risk in terms of their susceptibility to cybercrime.

This finding has some resonance with previous research that highlighted individuals in the 15–24 age group were more likely to be victims of cybercrime (Oksanen and Keipi, 2013). The authors for this research suggested that the reason for such an increase in susceptibility to cybercrime is related to the sheer level of exposure that such a group has to aspects of the digital environment. Younger individuals appear to be more likely to engage in aspects of interaction through online media, but lack the capacity to detect the risks related to such interactions (Oksanen and Keipi, 2013). Additional research from Bidgoli *et al.* (2016) also showed that undergraduate students were highly vulnerable to cybercrimes, with 34% of their participants stating that they had been victims of malware attacks. Critically it appears that this group obtains much of its knowledge and information related to cybercrime prevention from the media or individuals they know who have been attacked (Bidgoli *et al.*, 2016). Bidgoli *et al.* (2016) suggested that this process could in turn influence the reporting of such crimes, as well as the uptake of preventative measures. In order to prevent this, more targeted and effective campaigns targeting younger age groups must be designed, with a recommendation that further empirical work be conducted to explore the wider reasons for increased susceptibility in such groups.

Segmentation and impulsivity

We consider that the additional trait impulsivity measure provides an objective gauge of how such a variable fits into the underlying susceptibility to cybercrime. As noted in the introduction, previous research has been conducted which demonstrates a link between impulsivity and poor information security adherence (Egelman and Peer, 2015; Hadlington, 2017). In the context of our research, the findings do support original propositions made in the HO RICU (2015) report, insofar as trait impulsivity appears to be a key personality factor associated with susceptibility to cybercrime. Individuals in the B: Digitally Vulnerable group scored consistently higher on each of the three sub-scales for impulsivity, but particularly on the measure of Non-planning impulsivity.

Conclusion and suggestions for future research

At present times, the actual mechanisms related to how and why certain groups of individuals lend themselves to having higher susceptibility to cybercrime than others are still largely unknown. A more structured framework for approaching this issue could yield actionable intelligence that could be used in a number of key ways. In particular, the use of segmentation analysis on a regional basis would allow critical resources to be used in a more targeted way. This could be linked into the use of bespoke communication packages that are tailored to communicate specific threats that may link into the segmentation parameters. By pairing the segmentation analysis with other measurement tools there is also a potential to gain a more detailed insight into how susceptibility links into aspects including demographic variables and psychometrics. Presenting forces with the capacity to do this online through an email link also provides a cost-effective way of collecting data. Most police services employ customer segmentation tools and techniques as part of wider community engagement strategies, and the sophistication of such tools varies widely. By presenting an opportunity to unify this approach across forces, more consistent data can be collected as well, giving researchers a chance to move towards the unified framework as suggested earlier in this section.

References

Anwar, M., He, W., Ash, I. *et al.* (2017). 'Gender Difference and Employees' Cybersecurity Behaviors'. *Computers in Human Behavior* **69**: 437–443.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018

Bidgoli, M., Knijnenburg, B. P., and Grossklags, J. (2016). 'When Cybercrimes Strike Undergraduates'. eCrime Researchers Summit, eCrime, 42–51.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., and Huettel, S. A. (2014). 'An Abbreviated Impulsiveness Scale Constructed through Confirmatory Factor Analysis of the Barratt Impulsiveness Scale Version 11'. *Archives of Scientific Psychology* **2**(1): 1–12.

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

Furnell, S. and Clarke, N. (2012). 'Power to the People? The Evolving Recognition of Human Aspects of Security'. *Computers & Security* **31**(8): 983–988.

Furnell, S. M., Jusoh, A., and Katsabas, D. (2006). 'The Challenges of Understanding and Using Security: A Survey of End-users'. *Computers & Security* **25**(1): 27–35.

Hadlington, L. (2017). 'Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours'. *Heliyon* **3**(7): e00346.

Hadlington, L. and Parsons, K. (2017). 'Can Cyberloafing and Internet Addiction Affect Organizational Information Security?' *Cyberpsychology, Behavior, and Social Networking* **20**(9): 567–571.

Herath, T. and Rao, H. R. (2009). 'Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness'. *Decision Support Systems* **47**(2): 154–165.

HM Government. (2016). *National Cyber Security Strategy*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed 11 January 2018).

HO RICU. (2015). *Serious and Organised Crime Protection Public Interventions Model: Defining the Vulnerable Groups*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502960/Gov.uk_Serious_Organised_Crime_deck_vF.pdf.

McCormac, A., Zwaans, T., Parsons, K. *et al.* (2017). 'Individual Differences and information Security Awareness'. *Computers in Human Behavior* **69**: 151–156.

Mylonas, A., Kastania, A., and Gritzalis, D. (2013). 'Delegate the Smartphone User? Security Awareness in Smartphone Platforms'. *Computers & Security* **34**: 47–66.

Oksanen, A. and Keipi, T. (2013). 'Young People as Victims of Crime on the Internet: A Population-based Study in Finland'. *Vulnerable Children and Youth Studies* **8**: 298–309.

Parsons, K., Calic, D., Pattinson, M. *et al.* (2017). 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies'. *Computers & Security* **66**: 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). 'Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)'. *Computers & Security* **42**: 165–176.

Prensky, M. (2001). 'Digital Natives, Digital Immigrants Part 1'. *On the Horizon* **9**(5): 1–6.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). 'Analysis of End User Security Behaviors'. *Computers & Security* **24**(2): 124–133.

Downloaded from https://academic.oup.com/policing/advance-article-abstract/doi/10.1093/police/pay027/4970000
by guest
on 18 May 2018