Students' Cybersecurity Awareness at a Private Tertiary Educational Institution

Rajesh Chandarman
MCom Graduate, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Brett van Niekerk
Honorary Research Fellow, School of Management, IT and Governance, University of KwaZulu-Natal, Westville, Durban

Abstract

Internet-based attacks have become prevalent and are expected to increase as technology ubiquity increases. Consequently, cybersecurity has emerged as an essential concept in everyday life. Cybersecurity awareness (CSA) is a key defence in the protection of people and systems. The research presented in this article aimed to assess the levels of CSA among students at a private tertiary education institution in South Africa. A questionnaire tested students in terms of four variables: cybersecurity knowledge; self-perception of cybersecurity skills, actual cybersecurity skills and behaviour; and cybersecurity attitudes. The responses revealed several misalignments, including instances of "cognitive dissonance" between variables, which make the students potentially vulnerable to cyber-attacks. The findings demonstrate the need for targeted CSA campaigns that address the specific weaknesses of particular populations of users.

Keywords
cybersecurity awareness (CSA), password management, cyberbullying, phishing, malware, identity theft, pirated content

DOI: https://doi.org/10.23962/10539/23572

Recommended citation
Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication (AJIC)*, *20*, 133-155. https://doi.org/10.23962/10539/23572

1. Introduction

As is widely reported in the media, cyber-attacks are increasing in quantity and sophistication (Symantec, 2013). In most cases it is the weakest link in cybersecurity – the human element – that is the target for the increasing number of online criminals who are perpetrating an ever-greater variety of cybercrimes. The need for cybersecurity awareness (CSA) campaigns is thus undisputed, as these remain the first line of defence in providing employees and stakeholders with the know-how to interact safely online. International cybersecurity best practices advocate for CSA, and this filters into organisational policies and standards. An example in the education sector is the cybersecurity awareness campaigns and material provided by Educause (2017). Countries such as Australia, Canada, the UK and the US have implemented CSA campaigns supported by national committees and strategies (Cyber Aces Foundation, 2014; Office of Australian Info Officer, 2014; Rosewarne, 2013). Compared to these countries and others in Africa such as Mauritius and Kenya, South Africa has been found wanting in its CSA efforts (Doyle, 2015).

In South Africa, section 51(6) (g) of the draft Cybercrimes and Cybersecurity Bill specified that there is a need to (Minister of Justice and Correctional Services, 2015):

> (ii) promote and provide guidance in development and implementation of situational analysis and awareness campaigns concerning the risk environment of the South African cyberspace;
>
> (vi) cybersecurity training, education, research and development programmes amongst other initiatives.

For the purposes of this article, cybersecurity is defined as the protection of cyberspace itself, of the tangible or intangible technologies that support cyberspace, of electronic information, and of the users in their personal, societal and national capacities (Von Solms & Van Niekerk, 2013). Awareness is conceived of as comprising knowledge, self-perception of skills, actual skills and behaviour, and attitudes, and the inter-relationship among these elements.

In August 2014, it was reported that Russian cyber-criminals compromised 500 million email addresses and 1.2 billion passwords and usernames (*BBC News*, 2014). In April 2015 the names and social security numbers of approximately 280,000 AT&T US customers were sold to various third parties after being stolen by employees at call centres in the Philippines, Mexico and Colombia. As a result, AT&T was fined USD25 million by the US communications regulator, the Federal Communications Commission (Ruiz, 2015). In the same month, hackers allegedly from Islamic State compromised the social media pages and website of French television network TV5Monde, and disrupted the broadcasts of all 11 channels (Ashford, 2015).

The South African economy lost approximately ZAR1 billion in 2014 due to identity theft, of which there were approximately 4,000 reported cases (Compuscan, 2014). Insufficient awareness around cybercrimes is a possible reason for the South African Banking Risk Information Centre (SABRIC) reporting that over ZAR2.2 billion was lost in 2013 due to online fraud, identity theft and scams (*BusinessTech*, 2014).

Students are considered one of the computer-user profiles that is most vulnerable to cyber-attacks, as they are often careless and sometimes reckless in their computer usage and spend copious amounts of their time using technology (Aliyu, Abdallah, Lasisi, Diyar & Zeki, 2010). The persistent psychological need to remain connected via an increasing variety of electronic devices further exposes individuals to online risks (Mochiko, 2016).

There have been very few studies of CSA in South Africa, even fewer focusing on students attending South African public tertiary institutions, and, before this study, no studies of CSA among students at private tertiary institutions could be found. The research presented in this article, which was conducted for a Master's dissertation (Chandarman, 2016), sought to fill this gap by investigating the private tertiary students' online activity, and their knowledge, self-perception of skills, actual skills and behaviours, and attitudes, as they relate to cybersecurity issues. Among the aims of the research was to determine the degree of necessity of an intensive, focussed CSA training and education campaign tailored to the needs of the audience, as opposed to a general awareness campaign that is common to all audiences. The subject matter included in the survey, in order to evaluate the students' CSA, included: password management, cyberbullying, social engineering (including phishing and online scams and fraud), malware, identity theft, and general secure behaviour (e.g., downloading and sharing "pirated" film and TV content, using pirated software).

2. Literature review and analytical framework

An adapted version of the theory of planned behaviour (TPB) framework was used for the study. The TPB framework, originally proposed by Icek Ajzen, was found to be suitable because it has been used in investigating individuals' ethical behaviour and decisions in respect of adoption of, and compliance with, computer security measures (Ifinedo, 2012; Lee & Kozar, 2005; Leonard, Cronan, & Kreie, 2004). However, the TPB framework does not explicitly consider the case for CSA, and therefore it needed to be adapted. To adapt the framework, previous studies on CSA were considered, in order to determine necessary CSA variables and possible relationships among the variables. These earlier studies also formed a baseline against which the results of this study could be compared.

Furnell, Gennatou and Dowland (2002) found that organisations and individuals were unsure as to what they should be doing to improve their cybersecurity or how to achieve this, despite acknowledging that it was an issue that needed to be addressed.

The key to providing clarity, according to the National Institute of Standards and Technology (NIST, 2003), is CSA training and education. In addition to providing direction on security policies and how to properly use and protect IT resources and information, NIST SP 800-16 (1998) indicated that all employees in every organisation should have a basic literacy and awareness of information security. A range of topics for CSA training were suggested in NIST SP 800-50 (2003): data backup, malware protection, web usage, email and attachments, password usage and management, and social engineering.

A study by Rajan (2010) investigated the relationship between the likelihood of users falling victim to phishing (a form of social engineering which uses emails to maliciously solicit information from computer users, such as login or financial account details) and their awareness of the topic. The study concluded that people fell victim to phishing despite having knowledge and understanding of the importance thereof. This was attributed to incorrect behaviour patterns regarding online security. The use of simulated phishing emails to generate user awareness was investigated by Dodge and Ferguson (2006). Their study intended to assess the awareness levels of students at the United States Military Academy in order to inform their awareness programme. The study found that conducting the exercise, in addition to aiding them in tailoring their awareness drive, itself increased awareness. A similar study by Steyn, Kruger and Drevin (2007), focusing on higher education staff in the Western Cape Province of South Africa, found that email security considerations should be prioritised for education and awareness activities. These studies illustrate that *both* correct awareness and correct attitudes are essential in addition to knowledge in promoting secure behaviour online. Mishra (2014) found that many users exhibit a misperception that an installed anti-virus programme is sufficient to prevent compromise of their computers, and that a number believe that firewalls are the same as anti-virus applications.

An advanced cyber-espionage campaign employing both malware and social engineering to target governments, journalists and businesses in Southeast Asia and India over a 10-year period was discovered by FireEye in April 2015 (Lennon, 2015). The Heartbleed vulnerability was disclosed and made news headlines as the biggest security vulnerability in the history of IT in April 2014 (Mitre, 2014). Later that month, users were advised to use an alternative to Internet Explorer due to a severe vulnerability in the browser where malware could be unknowingly installed via webpages browsed (Rosenblatt, 2014). In September 2014 a number of distributed denial of service (DDoS) attacks and Botnet activity were recorded globally within an hour of the ShellShock/BashDoor vulnerability being disclosed (TroyHunt, 2014). These incidents illustrate the necessity of awareness regarding the need for patching and updating of machines, in addition to the need for awareness regarding phishing and social engineering, in order to protect against sophisticated attacks, ransomware, and other attacks.

A study by Pramod and Raman (2014) found that students in higher education are not ignorant of security concerns regarding smartphones, but at the same time are not fully aware of all the security risks and necessary security practices. Pretorius and Van Niekerk (2015) recommended training and awareness campaigns after finding vulnerabilities in industrial control systems due to users' insecure password management, unapplied software patches, and outdated or uninstalled anti-virus and malware protection. These studies further illustrate how there can be misalignment among cybersecurity attitudes, knowledge, and behaviour.

Victims of identity theft may suffer heavy consequences, including damaged credit scores and financial charges (Janssen, 2014). Wlasuk (2012) found that if identity information data held by higher education institutions was sold on the cyber black market, they would potentially be worth billions of dollars. A 2014 Kaspersky and B2B report found that South African Internet users generally had the misperception that cyber-criminals would see no value in their account credentials (*MyBroadband*, 2015). An exploratory study of college students by Mensch and Wilkie (2011) found that a false sense of security, in relation to personal information protection, is created by the installation of security applications and tools. Butler and Butler (2014) concluded that South Africans consider convenience a higher priority over security, and that only 23% of South African users regularly change their passwords despite 70% indicating that they are aware that this is good practice. These findings show that knowledge does not necessarily translate into good practice.

Kim (2014) found that many college students in the US did not participate in information security awareness training, even though they appeared to understand the need and importance of the training. Another finding of the study was that the students' security learning occurred piecemeal, from a number of sources, and that to develop sustainable secure behaviour they needed to participate more in focussed information security and awareness training. This again illustrates the potential for disconnections between good secure practice and having sufficient knowledge and understanding.

If security practices are too time-consuming or difficult, users will try to circumvent the controls in place, which may also reduce the effectiveness of previous and current awareness campaigns. Influencing strategies are required in addition to the knowledge transfer and awareness in order to positively alter behaviours and attitudes (Bada & Sasse, 2014). Peltier (2005) found that a baseline of the cybersecurity perception levels, attitudes, knowledge and skill, and the relationships amongst these, are required to guide the training.

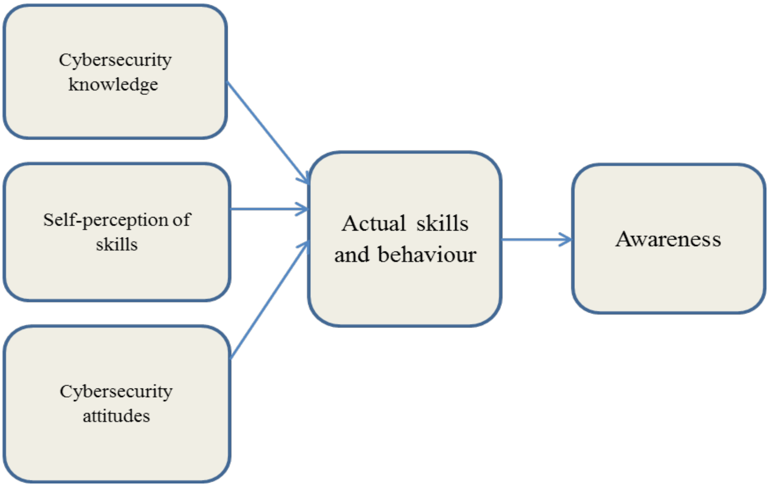
Hagen and Albrechtsen (2009) concluded that an e-learning tool that they assessed was a suitable mechanism for the initial creation of common values and attitudes to build a corporate information security culture. Kaur and Mustafa (2013) investigated how information security awareness of Malaysian small and medium enterprise employees was affected by attitude, behaviour, and knowledge. The study found that attitude and behaviour had significant relationships with information security awareness, but knowledge did not. This is consistent with the findings of Bada and Sasse (2014). Aliyu et al. (2010) found that, among Malaysian IT and education students, IT usage was affected by attitudes and perceptions towards computer ethics and security. Bakar, Chang and Saidin (2013) investigated e-commerce consumers' practices, knowledge and attitudes, and found that there was little knowledge or education regarding legal provisions, and that fostering better behaviours and attitudes was required to mitigate the likelihood of the consumers falling victim to cyber-criminals.

Aliyu et al. (2010) found that university students in Malaysia were major violators of computer ethics and security, as they were often reckless when posting content and browsing and were frequently involved in illegal usage via sharing and downloading of counterfeit software, TV series and movies. Due to a range of factors including laziness and economic standing, the students were found to not be practising safe computing in general (Aliyu et al., 2010).

The general consensus that emerges from the literature is that training and education are key initiatives to generate CSA and ameliorate poor online security behaviour. The studies considered in the literature also suggest that knowledge, self-perception of skills, actual skills and behaviours, and attitudes, are all relevant to assessing CSA, and that knowledge alone is typically not sufficient to ensure CSA, i.e., knowledge is often a weak variable.

Accordingly, our adapted version of the TPB framework investigated CSA via focus on relationships among four core variables: (1) *knowledge*, (2) *self-perception of skills*, (3) *actual skills and behaviour*, and (4) *attitudes*.

Figure 1: The TPB framework adapted to the CSA study



3. Methodology

The study followed an exploratory approach, using non-probability sampling. The study site consisted of three campuses of a private tertiary education institution in South Africa's KwaZulu-Natal Province, and a convenience sample of students was taken (i.e., those who attended lectures at an appropriate time for the researcher to gather data).

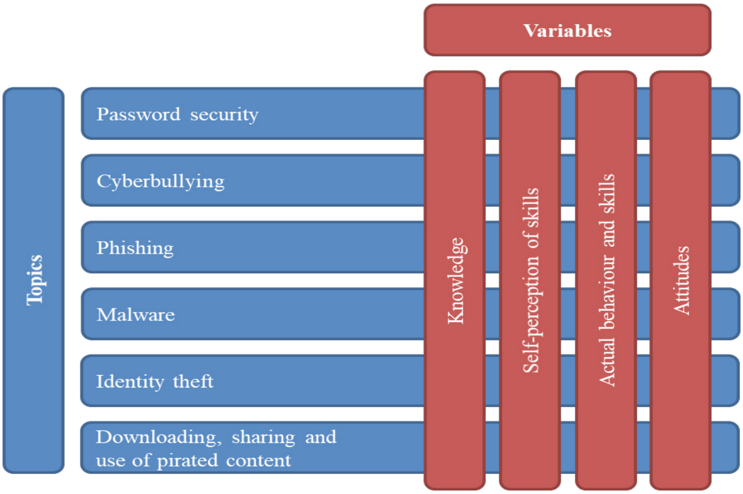
Data were collected via a questionnaire that received a total of 1,231 responses over two semesters (528 respondents online in the first semester, and 703 respondents for the paper-based questionnaire in a second semester). The results were analysed using the SPSS statistical software package, employing: descriptive statistics to assess individual topics and variables; Pearson Correlation and chi-square to assess relationships among variables; and Cronbach Alpha to assess significance.

A high-level outline of the questionnaire is as follows:

- section 1: The student's demographic information
- section 2: the student's online usage
- section 3: the student's cybersecurity knowledge
- section 4: the student's self-perception of cybersecurity skills
- section 5: the student's actual cybersecurity skills and behaviour
- section 6: the student's cybersecurity attitudes

The focus of this article is on the data generated by answers to questions in sections 3 to 6. Figure 2 below visualises the variables and topics considered.

Figure 2: Variables and topics in the study


Variables
Topics
Password security
Cyberbullying
Phishing
Malware
Identity theft
Downloading, sharing and use of pirated content
Knowledge
Self-perception of skills
Actual behaviour and skills
Attitudes

4. Findings

Cybersecurity knowledge

The "knowledge" category (section 3) offered students multiple-choice-format responses to factual questions regarding the six cybersecurity matters that were the focus of the research. Only one answer for each question was accepted as correct. The student responses were recoded numerically in binary fashion: as "2" if they answered the question correctly and "1" if they got the question wrong or indicated that they did not know answer. Frequency analysis was then conducted for the responses to each question. Figure 3 provides the frequency analysis.

Of note in Figure 3 are the significant lack of knowledge of what phishing is (56% answered incorrectly or did not know), and the significant lack of knowledge of the purpose of anti-virus software (43% answered incorrectly or did not know).

Figure 3: Students' knowledge of six cybersecurity matters
(N = 1188, 1197, 1193, 1191, 1182, 1196)

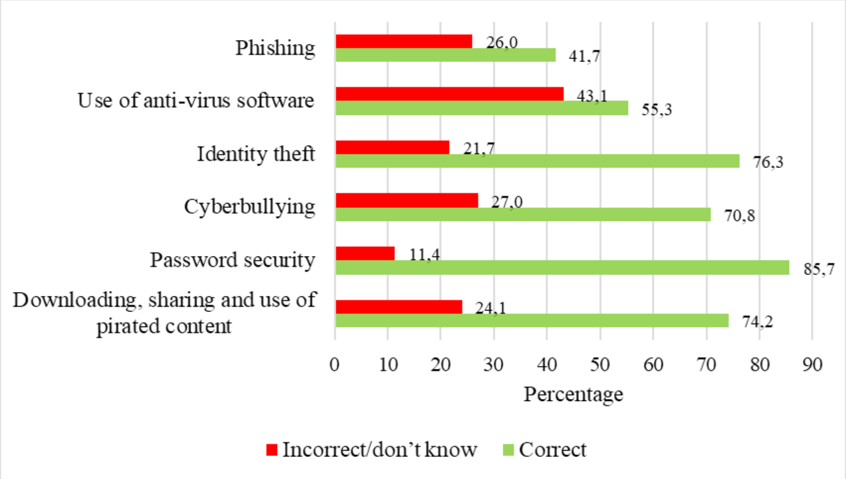


Table 1 below shows the section 3 responses prior to binary recoding. Approximately 38% of respondents selected "I do not know" for the phishing question, and 41% of respondents thought that anti-virus software was protection against "every possible attack".

Table 1: Cybersecurity knowledge before recoding (shown as % of responses)

3.1. What is phishing?	**%**
Unsolicited requests (spam) to fool receivers into divulging personal information	39.6
Disguised hyperlinks and sender addresses	6.1
Viruses being downloaded onto your devices	1.4
Your device being hacked to steal information	12.5
I do not know	37.9
Spoilt/blank	3.8
3.2. What is anti-virus software used for?	**%**
Disrupt and covertly steal information from your devices	0.7
Updating your software and systems	1
Protect your computer devices against malicious code	53.7
Preventing every possible attack on your computer devices	40.7
I do not know	2.3
Spoilt/blank	2

The findings shown in Table 1 suggest that that the respondents' knowledge levels in respect of phishing and anti-virus software were inadequate. Such knowledge deficits can lead to unsafe practices, and can be exploited by cyber-criminals.

Self-perception of cybersecurity skills

The results from the section 4 on self-perception of cybersecurity skills are presented in Table 2 below. The section consisted of six statements – one for each of the six cybersecurity matters that were the focus of the research – to which the respondent was asked to indicate her or his level of agreement based on a five-point Likert scale (1 = "strongly disagree", 5 = "strongly agree").

Table 2: Self-perception of cybersecurity skills

	N	Mean	Std. deviation	Std. error mean
4.1 I am confident I can identify a phishing email or a social engineering attack	1193	**3.19**	1.186	.034
4.2 I am adequately protected from malware, scareware and spyware	1197	**3.43**	1.059	.031
4.3 I am well liked and will never be a victim of cyberbullying	1207	**3.14**	1.152	.033
4.4 I do not post anything that will cause me to be a victim of identity theft	1207	**3.94**	1.030	.030
4.5 My passwords are strong enough. Nobody can guess them	1204	**3.95**	1.022	.029
4.6 Sharing downloaded (*) movies and TV series with my friends is OK	1206	3.03	1.228	.035

* "downloaded" in this context referred to content downloaded illegally without paying for it (i.e., "pirated" content)

A Cronbach Alpha test was done on the responses to all six statements, yielding a result of α = 0.668. Since this figure was less than 0.7, the test was therefore recalculated with question 4.6 excluded, resulting in an acceptable score of α = 0.707.

The first five statements generated a mean score > 3 and a p < .0005, indicating a significant level of agreement with the statements. Thus, overall, the students exhibited generally favourable self-perceptions of their cybersecurity skills. However, at the same time, four of the statements received a large percentage of neutral responses: the phishing (32%); malware, scareware and spyware (31%); cyberbullying (37%); and sharing downloaded movies and TV series (35%) statements. These neutral responses implied that the students in question had not developed an opinion or stance on these areas, suggesting a lack of comprehensive CSA.

Actual cybersecurity skills and behaviour

Table 3 below shows the seven scenarios respondents were asked to respond to in part B of section 5 of the questionnaire, which was focused on determining the students' actual cybersecurity skills and behaviour. Part B focussed on responses to scenarios, whereas Part A focussed on self-reporting of behaviour.

Table 3: Text of questions on actual cybersecurity skills and behaviour

5.11 You receive an email from your bank that your account needs to be verified because the bank has installed new software. You are required to click on a link provided and supply the necessary personal verification information. You must respond within the next 24 hours otherwise your bank account will be blocked and frozen. What do you do? a) Click on the link and provide the personal information requested so the security matter can be addressed without your account being frozen. b) Ignore it. It looks like a scam, so you delete the message without responding. c) You are suspicious but aren't sure if this is a scam or not. You respond to the text message, asking questions to determine if the situation. is legitimate before you provide the information requested. d) Phone the bank to check if this is true. e) Report the matter to the police.
5.12 I update my Windows/Apple, anti-virus, browser and other software: a) Once a month. b) When I remember. c) When I am reminded. d) Never.
5.13 The mouse cursor on your screen starts to move around on its own and click on things on your desktop. What do you do? a) Call someone so that they can see. b) Disconnect your computer devices from the network/ internet. c) Unplug your mouse. d) Turn your computer device off. e) Run your antivirus.

Table 3 (cont.): Text of questions on actual cybersecurity skills and behaviour

5.14 Your friend sends you an email with a screensaver they say you will love. What will you do?

a) Download it onto your device, since you trust your friend.
b) Forward the message to other friends to share it.
c) Call an IT professional and ask them to install it for you.
d) Delete the message.
e) None of the above.

5.15 "At campus yesterday, Josh was mucking around with a water spray gun and wet John's pants. It was hilarious because it really looked like John wet his pants and Tyson even got a photo! We were all joking about it and calling John 'Little Johnnie' and saying stuff like, 'Do you need your nappy changed, Baby John?' Then last night some of us got onto Facebook and we told everyone about it, and put the photo up too. Everyone said how funny it was, and they thought of some really funny things to tease John with today!" What is your opinion on this scene?

a) Hilarious.
b) Most people think this is funny
c) Hmm, made me laugh, but .. not sure if it was fair.
d) This hurt someone's feelings.
e) Yuck, this was deliberate and only done to hurt someone (emotionally and/or physically).

5.16 If someone searches for information about me on the internet, they would find:
i. My name
ii. My photograph
iii. My telephone number
iv. My home address
v. My bad habits (and things I would be embarrassed about)
vi. Pictures of my holidays
vii. My family members

a) All of the above.
b) 2 to 3 of the above.
c) 4 to 5 of the above.
d) A few of the above.
e) None of the above.

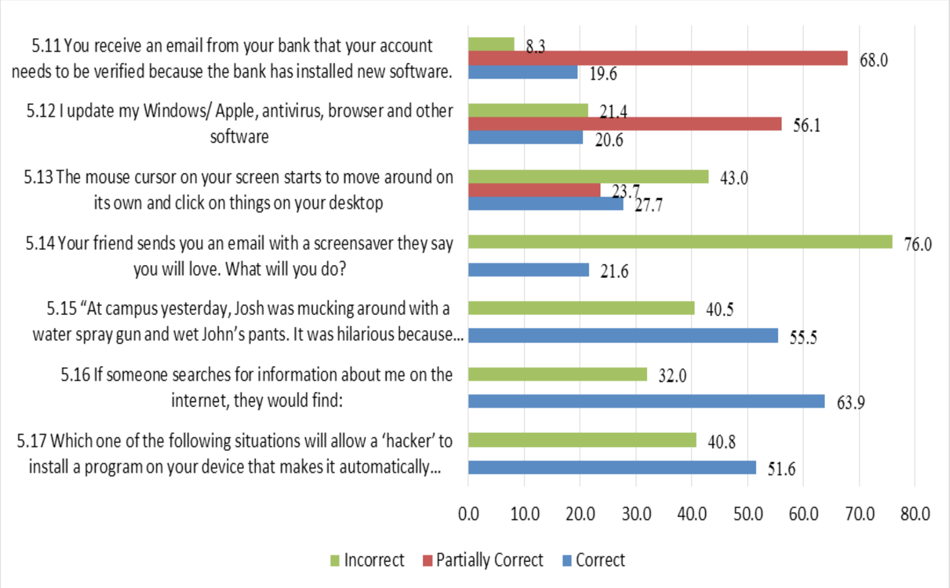
5.17 Which one of the following situations will allow a "hacker" to install a program on your device that makes it automatically send out tons of spam email from your device without your knowledge?

a) Out of date software patches.
b) No anti-virus installed or out of date anti-virus.
c) Clicking an unknown link or attachment.
d) Downloading unknown or unsolicited programs onto your computer device.
e) All of the above.

Figure 4 provides a summary of the frequency analysis for responses to each of the seven scenarios.

Figure 4: Actual cybersecurity skills and behaviour

(N = 1166, 1194, 1149, 1188, 1169, 1167, 1124)



Notable findings shown in Figure 4 are the large percentage (76%) of unsafe responses regarding opening a screensaver received from a friend (question 5.14), the large percentage (68%) of only partially correct (i.e., only partially safe) responses regarding response to a bank phishing email (question 5.11), and the large percentage (56.1%) of only partially correct responses to the question regarding updating of software (question 5.12). All these findings indicate unsafe cybersecurity skills and behaviour.

The Cronbach Alpha test was calculated, with questions 5.5 and 5.10 excluded as they were inverted, i.e. negative questions. For the remaining five questions, a result of $\alpha = 0.766$ was returned, indicating a high reliability. The Chi-square analysis (shown below in Table 4) for the whole group indicated that certain responses showed significant results. For example, the only partially correct responses for question 5.11 were significant ($\chi2$ (2, N = 827) = 765.666, $p < .0005$.

Table 4: Chi-Square results for cybersecurity skills and behaviour questions

Question	Result	N	df	Chi-square	p
5.11	partially correct (i.e., partially safe)	827	2	756.666	p < .0005 *
5.12	partially correct	683	2	306.226	p < .0005
5.13	incorrect (i.e., unsafe)	523	2	79.770	p < .0005
5.14	incorrect	925	1	368.892	p < .0005
5.15	correct (i.e., safe)	676	1	28.648	p < .0005
5.16	correct	778	1	129.667	p < .0005
5.17	correct	628	1	15.502	p < .0005

* SPSS reports a *p* of .000 as *p* < .0005

Cybersecurity attitudes

The responses to the questions on cybersecurity attitudes (section 6 of the questionnaire) are presented in Table 5 below. Generally the results were encouraging, as students indicated generally low levels of agreement with the statements, all of which were statements for which agreement would represent a potentially unsafe/harmful attitude. The one worrying exception was in the responses to question 6.1, where students exhibited an overly trusting view towards content sent via email from the email accounts of their friends – a level of trust that could make the receiver susceptible to malicious content.

Reliability for the eight questions in section 6 was tested using Cronbach Alpha, which returned $\alpha = 0.713$. It can therefore be concluded that the responses were consistent and a reliable measure of respondent attitudes towards the six cybersecurity matters.

Table 5: Cybersecurity attitudes

	N	Mean	Std. deviation	Std. error mean
6.1 My friends would not send me anything malicious or scams through email.	1170	**3.62**	1.122	.033
6.2 Updating my security software and Windows /Apple is too time consuming, annoying and uses up my bandwidth/ data bundle.	1168	2.69	1.122	.033
6.3 The security settings and tools slow me down and are pesky. I turn them off or disable them.	1166	2.39	1.004	.029
6.4 It is a waste of time to change passwords because you can still get hacked	1163	2.47	1.062	.031
6.5 It is too difficult to remember difficult passwords; therefore I use my name or something easy to remember.	1171	2.34	1.203	.035
6.6 Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their face.	1169	1.76	1.024	.030
6.7 It is OK to download (*) movies and TV series because the companies that make them are rich and I really cannot afford it (I am a student).	1169	2.53	1.143	.033
6.8 If I pirate software I will not get updates and security patches, but I don't need [updates and patches]	1162	2.29	.998	.029

* "download" in this context referred to downloading of "pirated" film and TV content (i.e., content acquired illegally, without the required authorisation obtained or payment made)

5. Analysis

Misalignments in relationships among CSA variables

With respect to phishing, correlation results illustrated weak negative relationships between student *self-perceptions of skills* and (1) their *actual skills and behaviour*, and (2) *attitude*, on the matter. This indicates that while the students had a favourable perception of their security protection and their skills in this area, their actual skills and behaviour, and attitudes, were not as safe as their perceptions implied they were.

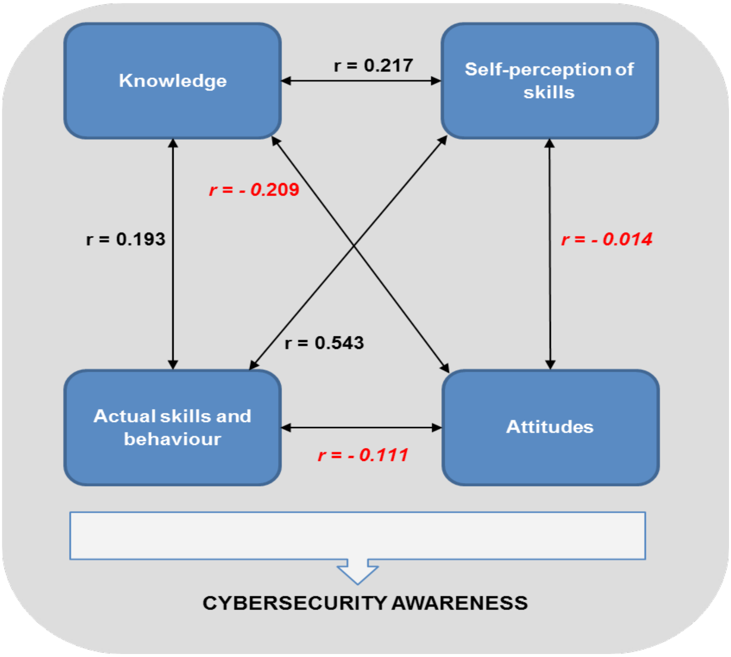
In respect of pirated content, while most students reported *actual skills and behaviour* suggesting they engaged in piracy, most at the same time also held the correct *attitude* towards pirated content, i.e., the attitude that it can be dangerous. This indicates students will engage in behaviour even though they know it is wrong.

Similarly, in respect of cyberbullying, despite a majority of students reporting favourable *self-perceptions of skills and behaviour* for avoiding cyberbullying behaviour when posting messages online, the majority also gave *attitude* responses indicating a potentially harmful attitude towards posting offensive pictures and messages.

For passwords, most students reported an *attitude* that it was difficult to remember complex passwords and so they used simple ones like their names (question 6.5), a potentially harmful attitude. Yet, at the same time, for the majority, the *self-perceptions of skills and behaviour* suggested they had strong passwords (question 4.5), results in the negative correlation (r = -.196, p < .0005). These are clear contradictions and disconnects among responses to the CSA variables.

To determine general correlations between the four variables – knowledge, self-perception of skills, actual skills and behaviour, attitudes – based on data from all the questions on the six cybersecurity topics, Pearson Correlation Coefficients were calculated for each, as presented in Figure 5.

Figure 5: Relationships between variables



It can be seen in Figure 5 that there are positive correlations amongst *knowledge*, *self-perception of skills*, and *actual skills and behaviour*. The strongest positive correlation is the relationship between *self-perception of skills* and *actual skills and behaviour*, with the other correlations having relatively low values. This indicates that *knowledge*, *self-perception of skills*, and *actual skills and behaviour*, have positive, albeit small, impacts on each other. Meanwhile, all three of these variables are negatively correlated with *attitudes,* which is to say that: the more correct the *attitudes*, the lower the levels of *knowledge*, *self-perception of skills*, and *actual skills and behaviour* appear to be. The strongest negative correlation is between *knowledge* and *attitudes,* indicating that poor knowledge results in a good attitude, or vice versa. These negative correlations indicate a form of cognitive dissonance.

The dilemmas of cognitive dissonance on CSA matters

We saw above, in the "Findings" section and in the first part of this "Analysis" section, that: there are shortcomings in some areas of the students' cybersecurity *knowledge*, *actual skills and behaviour*, and *attitudes;* and in some of the cybersecurity areas for which the majority of students had strong *self-perception of skills,* the majority at the same time showed evidence of weak *actual skills and behaviour*, which implies a false sense of security. This misalignments and disconnects are concerning, and they were exhibited, in particular, in respect of the topics of (1) cyberbullying, (2) password security, (3) identity theft, and (4) phishing. It is thus evident that there are shortcomings in the CSA of many of the private tertiary students surveyed.

One of the most concerning results in the *knowledge* category (see Figure 3 and Table 1) was that over half of the students reported a weak understanding of phishing. And adding to the worrying nature of this finding was the fact that, at the same time, the majority of students gave a contradictory *self-perception* answer on the same topic, by indicating they are confident in being able to identifying a phishing email. This finding aligns to findings of the study by Kaur and Mustafa (2013), which concluded that there is no significant relationship between knowledge and true information security awareness. Similarly, Bada and Sasse (2014) reported that knowledge alone is insufficient for true awareness. Phishing attacks are becoming more prevalent, resulting in increased media attention on the topic, and increased attempts at education and awareness. Yet the CSA messaging in respect of phishing does not seem to be reaching the students, or they are ignoring it. This situation is precarious, as the results indicate the students have a false sense of security, which may make them more susceptible to falling victim.

Parbanath (2011) found that consumers exhibited a large degree of concern over the disclosure and protection of their personal information, yet at the same time, in contradictory fashion, had limited knowledge of the relevant legislation. The students surveyed in this research appeared to exhibit an analogous contradiction: concerned about phishing yet not managing to acquire the necessary knowledge. This confirms that knowledge alone is not enough, and that it needs to be combined with training, as in the phishing simulation exercise by Dodge and Ferguson (2006).

The majority of students professed to the correct *actual skills and behaviour* on phishing by agreeing that they will not open suspicious email attachment, which corresponds to their *self-perception* that they can identify phishing attempts. But as discussed above, this does not correspond with their knowledge. Rajan's (2010) study found that those with knowledge and understanding of phishing still fell victim. And in spite of the widespread attention that phishing has received in recent years, a 2014 study by the University of California and Google reported that phishing attempts still succeeded 45% of the time (Beres, 2014).

The students surveyed seemed clearly to have a false sense of security. In the *actual skills and behaviour* section of the questionnaire, some of the answers provided were partially correct (e.g., the students would verify with the bank regarding a suspicious email). However, South Africa's banks, and awareness initiatives by SABRIC (2015), have clearly indicated that banks will not request details by email. Therefore the most clearly correct answer was to ignore and immediately delete the email.

Another worrying result was that over 40% of the respondents gave the view, in the *knowledge* section of the questionnaire (see Table 1), that an anti-virus program is sufficient protection against all possible attacks, and that, accordingly, they were well protected while online. This finding is consistent with Mishra's (2014) study, which reported that most computer users consider anti-virus software as adequate protection and think that firewalls and anti-virus software are the same (though modern Internet security applications do often include firewall functionality). Mensch and Wilkie's (2011) findings also indicated that a false sense of security may be gained by the installation of security tools, when in fact there is still vulnerability to other attacks such as identity theft and phishing.

In addition to their positive *self-perceptions of skills* in respect of phishing and anti-virus tools, the students also exhibited confidence in the strength of their passwords. Yet the students reported that it is too difficult to remember complex passwords so they stick to easy ones, and that they find changing passwords a waste of time. These are insecure behaviours. NIST SP 800-50 (2003) recommends regular changing of passwords, different passwords for different systems, as well as a minimum degree of password complexity. This should be enforced by CSA training (McCrohan, Engel, & Harvey, 2010). On a more positive note, the students confirmed their passwords should be kept secret. This contradicts the findings from the study by Steyn, Kruger and Drevin (2007), who found that over half the staff surveyed were happy to give out their passwords. As Steyn, Kruger and Drevin's (2007) study is more than 10 years old, we can perhaps assume that there has been some improvement in awareness of the need to keep passwords secret. Combined with the fact that the students considered it unacceptable to use the institution's network for messaging and social media, it could also indicate a link to heightened desire for privacy or secrecy.

The students also generally indicated positive *self-perception* in respect of not allowing themselves to fall victim to cyberbullying. However, research has found that sometimes perpetrators do not realise their actions are cyberbullying, and, at the same time, incidents often go unreported by the victims (Oosterwyk, 2010). This may to some extent explain the respondent students' perception that they would not fall victim to cyberbullying.

Overall, positive *self-perceptions* were reported by the students for the various cybersecurity issues. Such confidence is misplaced when not linked to correct *knowledge*, *actual skills and behaviour*, and *attitudes.*

In respect of *actual skills and behaviour*, the responses indicated that the students allowed for system and anti-virus updates, downloaded from reputable sites, checked their privacy settings, and were careful about entering personal information and what they posted online. These results indicate secure behaviour, which is consistent with Pramod and Raman's (2014) study which found tertiary education students are familiar with broad security issues. However, at the same time, there was a high percentage of incorrect responses for skills in dealing with suspicious files (76%) and dealing with situations when a hacker gains access to a computer (43%).

For the *attitudes* category, the most significant and strongest result was that students agree that they would not receive scams or malicious emails from their friends. This is a potentially harmful attitude, as most friends share jokes and funny/interesting videos and images with family and friends, and these attachments are possible delivery mechanisms for malware. Malware could thus be unwittingly transmitted. Therefore this trust is misplaced. Also in respect of attitudes, the students correctly disagreed with the statements: that it is acceptable to post offensive pictures and bad messages about their peers; that it is time-consuming and annoying to update security software; that they turn off security settings; that patches and updates are not required; and that it is acceptable to download movies. The rejections of these statements represent appropriate cybersecurity *attitudes*. However, several of these responses do not align with the students' *actual skills and behaviour*. It would seem that, to some extent, the students know what the acceptable norms are, but are willing to forgo following many of the norms at personal level. This is one of several instances of apparent cognitive dissonance revealed by the findings.

6. Conclusions

Cognitive dissonance in respect of cybersecurity matters – of the sort displayed by the students who were the respondents in this research – is a phenomenon that is targeted by cyber-criminals (Kritzinger & Von Solms, 2010), indicating that the students are vulnerable to cyber-attacks.

The number of potential victims can be reduced by increasing CSA (Department of Communications, 2013), making cybercrime less profitable. This cognitive dissonance found to be present among the students is a vulnerability that cyber-criminals exploit regularly, and indicates the need for a targeted CSA intervention to address the shortcomings of the specific population. The findings also suggest that generic awareness campaigns are no longer sufficient, and that an assessment of a target population is required to first identify the population's CSA shortcomings prior to designing the awareness campaign.

As CSA is a common issue affecting all computer and Internet users in South Africa, awareness levels in the country need to be assessed by surveying a large spectrum of the population. In order to achieve a baseline of CSA in South Africa, a "generic" CSA survey should be designed to be applicable across population segments, organisations, demographics and economic groups. The baseline data can be used over a period of time in larger longitudinal studies to monitor the effectiveness of implemented CSA initiatives. Deeper qualitative studies in CSA, investigating the underlying reasons and motives for specific users' knowledge, self-perceptions, actual skills and behaviour, and attitudes, also need be conducted to enhance understanding of the inter-relationships among these variables within various population segments.

Acknowledgements

This article is published as an extension to the first author's Master's dissertation (Chandarman, 2016).

References

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13-14 December. https://doi.org/10.1109/ict4m.2010.5971884

Ashford, W. (2015, April 10). French TV5Monde network cyber attack the latest in destructive trend in system intrusions. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/4500244107/French-TV5Monde-network-cyber-attack-the-latest-in-destructive-trend-in-system-intrusions

Bada, M., & Sasse, A. (2014). *Cyber security awareness campaigns Why do they fail to change behaviour?* Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Bakar, E. A., Chang, L. L., & Saidin, A. Z. (2013). Knowledge, attitude and practices of consumers in e-commerce transactions. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 5th International Conference. Rabat, 26-27 March. https://doi.org/10.1109/ict4m.2013.6518903

BBC News. (2014, August 6). Russia gang hacks 1.2 billion usernames and passwords. Retrieved from http://www.bbc.com/news/technology-28654613

Beres, D. (2014, July 11). Google study finds email scams are more effective than you'd expect. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/11/07/phishing-scams_n_6116988.html

BusinessTech. (2014, September 14). Internet fraud and phishing costs SA R2.2 billion. Retrieved from http://businesstech.co.za/news/general/68212/sa-internet-fraud-and-phishing-costs-r2-2-billion

Butler, R., & Butler, M. (2014). An assessment of the human factors affecting the password performance of South African online consumers. In N. Clarke, & S. Furnell (Eds), *Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2014)* (pp. 150-160), Plymouth, UK, 8-9 July.

Chandarman, R. (2016). *Cybersecurity awareness of students at a private higher education institute in South Africa*. Master's dissertation, University of KwaZulu-Natal, Westville, Durban.

Compuscan. (2014). Identity fraud on the increase. Retrieved from https://www.compuscan.co.za/identity-fraud-increase

Cyber Aces Foundation. (2014). US cyber challenge: Cyber quests April 2014. Retrieved from http://uscc.cyberquests.org

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security 29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Department of Communications (DoC). (2013). *Review report: E-commerce, cybercrime and cybersecurity – status, gaps and the road ahead*. Pretoria: Government of South Africa. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Review_Report_e-commerce_cybercrime%20and%20cybersecurity_final_0.pdf

Dodge R. C., & Ferguson A. J. (2006). Using phishing for user email security awareness. In S. Fischer-Hübner, K. Rannenberg L. Yngström. & S. Lindskog (Eds.), *Security and privacy in dynamic environments*. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May, Karlstad, Sweden. https://doi.org/10.1007/0-387-33406-8_41

Doyle, K. (2015, May 19). SA security policy trails Africa. *ITWeb*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=143303

Educause. (2017). Awareness campaigns. Retrieved from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357. https://doi.org/10.1108/09576050210447037

Hagen, J. M., & Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security, 17*(5), 388-407. https://doi.org/10.1108/09685220911006687

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Janssen, C. (2014). *Techopedia*. Retrieved from http://www.techopedia.com/it-dictionary

Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In IEEE (Ed.), *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). https://doi.org/10.1109/icriis.2013.6716723

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security, 22*(1), 115-126. https://doi.org/10.1108/imcs-01-2013-0005

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement, *Computers & Security, 29*(8), 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Kyobe, M., Matengu, S., Walter, P., & Shongwe, M. (2012). Factors inhibiting recognition and reporting of losses from cyber-attacks: The case of government departments in the Western Cape Province of South Africa. In N. Tadgh (Ed.), *6th European Conference on Information Management and Evaluation* (pp. 159-167). Reading, UK: ACP.

Lee, Y., & Kozar, K. (2005). Investigating factors affecting the anti-spyware system adoption. *Communications of the ACM, 48*(8), 72-77. https://doi.org/10.1145/1076211.1076243

Lennon, M. (2015, April 12). FireEye uncovers decade-long cyber espionage campaign targeting South East Asia. *Security Week*. Retrieved from http://www.securityweek.com/fireeye-uncovers-decade-long-cyber-espionage-campaign-targeting-south-east-asia

Leonard, L. N. K., Cronan, T. P., & Kreie, J. (2004). What are influences of ethical behaviour intentions – planned behaviour, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-58. https://doi.org/10.1016/j.im.2003.12.008

Malandrino, D., Scarano, V., & Spinelli, R. (2013). How increased awareness can impact attitudes and behaviors toward online privacy protection. In IEEE (Ed.), *2013 International Conference Social Computing (SocialCom)* (pp. 57-62). https://doi.org/10.1109/socialcom.2013.15

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security, *Journal of internet Commerce, 9*(1), 23-41. https://doi.org/10.1080/15332861.2010.487415

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information & Management Sciences Journal, 14*(2), 91-153.

Minister of Justice and Correctional Services. (2015). *Cybercrimes and Cybersecurity Bill.* Draft for public comments. Republic of South Africa.

Mishra, U. (2014). Is anti-virus a necessary evil? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434470

Mitre. (2014, April). The Heartbleed Bug. Retrieved from http://heartbleed.com/

Mochiko, T. (2016, November 22). Cybercrime "will rise" with internet of things. *Business Live*. Retrieved from https://www.businesslive.co.za/bd/life/gadgets-and-gear/2016-11-22-cybercrime-will-rise-with-internet-of-things

MyBroadband. (2015, April 22). South Africans underestimate password value. Retrieved from http://mybroadband.co.za/news/security/124870-south-africans-underestimate-password-value.html

National Institute of Standards and Technology (NIST). (1998). *Information technology training requirements: A role-and performance-based model*. NIST Special Publication 800-16. Washington, DC: US Department of Commerce.

NIST. (2003). *Building an information technology security awareness and training program*. NIST Special Publication 800-50. Washington, DC: US Department of Commerce.

Office of the Australian Information Commissioner (OAIC). (2014). Privacy Awareness Week resources 2014. Retrieved from http://www.oaic.gov.au/news-and-events/privacy-awareness-week-2014/resources-2014#training

Oosterwyk, G., & Parker, M. (2010). Investigating bullying via the mobile web in Cape Town schools. Paper presented to the 2010 Annual Conference on WWW Applications, Durban, South Africa, 22-24 September. Retrieved http://www.zaw3.co.za/index.php/ZA-WWW/2010/paper/view/239

Parbanath, S. (2011). *Personal information security: Legislation, awareness and attitude*. Master's dissertation. University of KwaZulu-Natal, Westville, Durban.

Peltier, T. R. (2005). Implementing an information security awareness program. *Information Systems Security, 14*(2), 37-49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133-19144.

Pretorius, B., & Van Niekerk, B. (2015). Cyber-security and governance for ICS/SCADA in South Africa. In J. Zaaiman, & L. Leenen (Eds.), *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 241-251). Reading, UK: ACP.

Rajan, M. (2010). *Internet phishing hook, line and hopefully not sunk*. MBA thesis, University of KwaZulu-Natal, Durban.

Rosenblatt, S. (2014, April 28). Stop using Microsoft's IE browser until bug is fixed, US and UK warn. *CNET*. Retrieved from http://www.cnet.com/news/stop-using-ie-until-bug-is-fixed-says-us

Rosewarne, C. (2013). *2012/3: The South African cyber threat barometer*. Retrieved from https://www.wolfpackrisk.com/research/south-african-cyber-threat-barometer

Ruiz, R. (2015, April 8). F.C.C. fines AT&T $25 million for privacy breach. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2015/04/08/f-c-c-fines-att-25-million-for-privacy-breach/?ref=topics

South African Banking Risk Information Centre (SABRIC). (2015). Website. Retrieved from https://www.sabric.co.za

Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity theft – empirical evidence from a phishing exercise. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. Von Solms (Eds), *New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the IFIP TC 11 22nd International Information Security Conference (SEC 2007)* (pp. 193-203). https://doi.org/10.1007/978-0-387-72367-9_17

Symantec. (2013). *2013 Norton report: Cost per cybercrime victim up 50 percent*. Retrieved from http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01

TroyHunt. (2014). Everything you need to know about the Shellshock Bash bug. Retrieved from http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wlasuk, A. (2012, June 29). Higher education – the perfect security storm. *Security Week*. Retrieved from http://www.securityweek.com/higher-education-perfect-security-storm