Accounting and Management Information Systems
Vol. 15, No. 1, pp. 112-130, 2016

Students' awareness on information security between own perception and reality – an empirical study

Victoria Stanciu [a] and Andrei Tinca[1a]

[a] *Bucharest University of Economic Studies, Romania*

ABSTRACT: The accounting profession is evolving aiming at responding in an adequate manner to the society's requirements dominated by the IT insertion in all the aspects of the life. The IT knowledge and skills needed by the accounting professionals are increased and the accounting faculties are determined to respond to the new professional requirements. This paper discusses the accounting students' awareness in regard with information security. The research performed emphasized the significant gap between the students' perception on their information security awareness and the reality. The study revealed that the students' computing knowledge is more technical and less addressed to information security issues. The research conclusions emphasize the urgent need for improving the universities' curriculum in regard with information security issues and students' training using information security awareness programs. The Romanian literature is scarce in regard with this topic. From this perspective, the present paper signals the need to deepen the students' training process aiming at better preparing the students for the professional life and make them be more employable.

Keywords: *IT Security, University Education, Employment Skills, IT Risk Awareness*

JEL codes: A2, M41, M15

[1] *Corresponding authors*: Andrei Tinca, Department of Management Information Systems, Bucharest University of Economic Studies, Piața Romana 6, 010374 - Bucharest, tel. (+40)21319100. email addresses: victoria.stanciu@cig.ase.ro, andrei.tinca@gmail.com

1. Introduction

The present is characterized by an increasing mingling of the IT field in the entire social, economic, financial and personal life. Our ecosystem has become a digital one, providing rapid connection between entities (like institutions and companies), people and data (EY, 2014), and promoting IT solutions in all the aspects of our work and life. Competition and performance imply rapid alignment to the IT paradigm. The companies' businesses are IT-based being changed the business models, the business strategies and the employees' daily activities and needed skills and abilities. The large and rapid adoption of mobile computing, cloud computing, and Internet of things has determined the blurring of the companies' boundaries. Mobile computing has immerged in the individuals' life too, generating a visible dependence and changed behavior in relation with these devices.

The speed registered in the information technology integration in the companies' life has not been always followed by rapid and solid information security and privacy measures. There is an evident gap between the companies' declared awareness regarding IT risks and their actions. The companies are not moving fast enough to face, in an effective manner, the expanding IT thereat landscape - a fact shown by the massive security breaches (PWC, 2014). The global survey performed in 2013 by PWC on information security revealed that 32% of the respondents are very or somewhat (39%) confident that in their companies the information security activities are effective (idem).

The information security problem became a major priority not just for the information security experts, but also for a large community including companies' managers and universities' staff. The universities' concern is related to the need to create the IT risk awareness among students and stimulate their thinking in regard with information security risks. This is a new requirement imposed by the IT environment they are going to face in the professional life.

This paper intends to present the authors' research conclusions in regard with the students' awareness related to information security. The present research is part of a larger project that includes the investigation of the companies' attitude and reaction towards IT threats and the IT users' knowledge, behavior and attitude regarding information security risks. Aiming to analyze how well the accounting students are trained and prepared to face information security threats, the authors conducted a survey in Romania's biggest faculty of accounting, the Faculty of Accounting and Management Information Systems, in the Bucharest University of Economic Studies. The survey conclusions represent valuable inputs for the university's curriculum improvement and development of security training programs for students. The Romanian literature is scarce in regard with this topic.

From this perspective, the present paper provides an important point in the Romanian economic universities' effort to permanently update their training process and curriculum aiming at responding to the new professional life requirements and improve their students' readiness to face it and be more employable.

2. Literature review

Cyber threats have no boundaries and their landscape is rapidly expanding. The companies' appetite for emerging technologies adoption is not determining rapid implementation of adequate information security measures aiming at mitigating potential risks. Even if the emerging IT solutions provide means to protect user's information and privacy, the technology by its self cannot provide effective information security. "Risks are neither well understood or nor properly addressed" emphasizes the global 2013 survey performed by PWC (PWC, 2013). And what is concerning is the same survey's conclusion, stating that "senior executives frequently are seen as part of the problem, rather than keys to the solution" (idem).

To ensure an effective security the companies have to adopt a proactive approach in information security and become more reactive in regard with the IT risks (EY, 2014). There is an increase of the attacks and the information security specialists recognize their sophistication. A survey performed in 2014 in UK revealed that 10% of the organizations experienced security breaches "were so bat affected that they had to change the nature of their business" (PWC, 2014).

The information security specialists emphasize that we are faced with an increase in opportunistic attacks that are exploiting weaknesses or vulnerabilities detected (Kim & Eyon, 2014). The employees' attitude and behavior represents one of the weaknesses. The survey performed in UK in 2014 revealed that 31% of the worst security breaches were caused by inadvertent human errors and 20% of them were generated by deliberate misuse of systems by staff (PWC, 2014). The companies can enforce the most adequate policies and information security actions, but as long as the employees are not trained in regard with these policies and they do not achieve a real awareness regarding IT risks and remain in compliance with the IS (information security) policies, the companies continue to remain less protected. Rastogi and von Solms underline this fact also emphasizing that he success of the security measures hinges on the end-users actions (Rastogi & von Solms, 2012).

The NIST SP 800-16 document underlines the importance of awareness, training and education of the people in regard with IS and recommends that IT security awareness programs should be aimed at changing the employees' security attitude and organizational culture (NIST, 1998). The Organization for Economic Co-

operation and Development (OECD) guidelines are addressing the security awareness and define the goal of security awareness underling that "participants should be aware of the need for security of information systems and networks and what they can do to enhance security" (OECD, 2002).

The lack of IS proactive ongoing training in the companies is emphasized by another survey performed in 2011 (Dimensional Research, 2011). The importance of ISA (Information Security Awareness) for the effectiveness of the security policies and controls is emphasized by the standards (ISO/IEC 27001, ISO/IEC 27002: 2005). Drtil emphasizes that companies aiming to avoid security incidents should take into consideration "cooperation not only in technological area, but also across strategic, process and organizational area" (Drtil, 2013: 1).

Romanian universities have developed IT platforms dedicated to support the administrative universities' activities and educational process. The students can access these systems having limited or larger access rights according with the platforms they are logging on. As authorized user they had to be trained in regard with the security policy so that to remain in compliance with the security rules and measures. On the other hand, universities have to train the students for their professional life, which is now significantly impacted by IT. Stanciu and Bran emphasize that in the Romanian universities' economic faculties' curriculum (accounting faculties inclusively), with small exceptions, there is a limited time allocated to computing lectures and labs. The lectures focus, mainly (for the bachelor level), on basic computing and databases and there is not much room for information security training (Stanciu and Bran, 2015). Eyon underlines that "students may be technologically well informed but it does not mean that they know to protect their information and systems effectively" (Eyon, 2014: 1). In this respect, Eyon recommends periodically measurement of the students' information security awareness and comprehensive training programs performed in the universities (idem). Eyon remains aligned to Green's opinion, which considers that information security should be considered a leading computing issue to address by the high education institutions (Eyon, 2013). Eyon recommends that information security training be offered during the students' first semester in college (idem).

The authors conducted an investigation in the Faculty of Accounting and Management Information Systems on the undergraduate students in regard with their awareness to information security risks. The methodology followed in our research and the main conclusions are stated in the next sections.

3. An overview of the current IT risk environment

We felt it is important to expand the literature review beyond the usual scientific sources, in order to describe the current IT risk climate. In this section we relied on trusted industry data to review significant incidents and reveal expert opinions. Thus we attempt to provide a more complete background for our research.

Cisco (one of the largest manufacturers of network equipment) states in its 2014 Annual Security Report that:

> *"The exploitation of trust is a common mode of operation for online attackers and other malicious actors. They take advantage of users' trust in systems, applications and the people and businesses they interact with. [...] There is ample evidence that adversaries are coming up with new methods for embedding their malware in networks, remaining undetected for long periods, and stealing data or disrupting critical systems […] (Within companies) threat alerts grew 14% year over year."* (Cisco 2014 Annual Security Report)

According to the report, the key vector of attack is the exploitation of users' trust. This is carried out mostly by *phishing* attacks—which are targeted e-mails with malicious content. Another researcher opines that "All it takes is for one user to open a file or click on a link […] and your network integrity is compromised" (Birtstone, 2015).

Another factor conductive to cyber-crime is the reduction of IT budgets in the corporate sector, leading to security loopholes, which are exploited by hackers (Dunkley, 2015). Banks are affected by the increased usage of mobile devices, which are outside their control (idem). An incident resulted in over $300 millions stolen from bank accounts, using malware (Sanger & Perlroth, 2015).

Hackers use stolen e-mail addresses to send spam and propagate malware. In 2015, three hackers were charged with stealing over 1 billion e-mail addresses—"one of the largest data breaches uncovered in U.S. history" (Dunsmuir and Finkle, 2015). The incident included clients of reputable banks such as Citigroup Inc. and JP Morgan Chase & Co.

High-profile hacking incidents impact corporations' stock prices. In 2015, Gemalto (a leading manufacturer of secure cards) lost $500 million from its stock price, after sensitive card data was stolen from its servers (Leyden, 2015). Sony Pictures was the victim of a major hacking incident, with the fallout affecting entire industries (Leyden, 2014).

Cloud applications are also targeted, with a report finding that only one in ten cloud applications are secure enough for enterprise use, and 15% of login for business applications could be compromised by hackers (Cooldige, 2015).

As entire sectors become more dependent on information technology, other types of incidents happen—beyond the "usual" bank hacks. Goodman states that:

> *"In California, 450 convicts were released from jail after a system error, while in the UK police computers wrongly branded 20,000 innocents as criminals. […] blind faith in computers could lead to the manipulation of everything from airport scanners to electronic voting."* (Goodman, 2015)

4. Methodology

The survey aimed to assess the accounting students' awareness in regard with security information was performed during February 2015. The survey's subjects were third year students of the Accounting and Management Information Systems Faculty in the Bucharest Academy of Economic Studies. The study focused on the third year students taking into consideration that in 6 months they became bachelors in accounting and new entry in the profession. We collected a total of 67 answers, representing approximately 33,67% of a population of 199 accounting students; thus the data should be significant for the whole population. The questionnaire included 22 items; out of which 19 examine students' attitudes and perceptions toward information security and 3 items were added for the demographic information. All respondents had prior experience in using Internet. The data analysis was conducted starting in line with the following hypotheses:

H1: *Students are aware of the current climate regarding information security threats and their attitudes have modified accordingly.*

We evaluate this hypothesis in light of the current heightened exposure that information security gathers in the international media an on-line environment where the students interact (Facebook, Google, Yahoo) and we attempt to gauge whether the students are receptive to the current risk environment.

H2: *Students express a need for more training in information security.*

According to (Eyon, 2014), information security training should be offered in the first college semester. We intend to measure whether our population fits these findings, with an interest to modify the school curricula accordingly.

H3: *Students who know what a phishing attack is, are less prone to security incidents*.

Phishing attacks are among the most dangerous attack vectors, and users are easily baited (Leyden, 2014). We look to prove the positive correlation between awareness and better protection. Since the students in our sample will soon be employed, we felt that this topic is relevant for the protection of the employer's assets.

H4: *Although students state that they are concerned about privacy, they share private data on-line.*

There is ample evidence of compulsive social network usage among students, with consequential privacy impact. Still, students share data with little regard to possible future implications such as employment background checks. The hypothesis aims to gather evidence for the introduction of topics regarding privacy in the scholar curricula.

H5: *Students posses self-confidence regarding information security, which is at odds with their real-world skills.*

Prior research shows that students are technologically literate but posses little knowledge to help them protect assets (Eyon, 2014). We attempt to test whether these technical abilities result into an inadequate perception of security awareness.

The survey's conclusion will be considered in the reviewing process of the academic curriculum aiming at improving students' preparedness for the professional life requirements. In the next phases of the research, the investigation will be extended over the entire population of accounting students.

4.1 Information security survey

We based our study on a survey, which we administered to undergraduate students in our university. The survey was constructed to test the stated hypotheses in terms of the following objectives:

- Gauge the student's perception regarding current security threats; we wanted to know if the students are aware of the current climate and if they perceive what risks they will face in their future jobs as accountants/auditors;
- Determine if the students *think* they have the necessary skills regarding computer security. Do they feel prepared, and do they feel they have enough information?

- Determine if the students feel a need to be trained in the IT security area, and whether this will help them in their future jobs. We also ask who they perceive should be responsible for their information security education;
- Find out what *real* security measures they use to protect their personal computers;
- Evaluate their perceived level of competence against a set of well-known security practices.

The topics investigated by the surveys' questions are inspired by the most frequent and destructive malicious attacks registered in the last years (some being presenting in the sections above) and included in the security reports issued. We also took into consideration, the specialists' opinion in regard with the need to periodically assess the students' information security awareness (Eyon, 2013).

4.2 Sample characteristics

In our sample, 93% of the respondents were female, which is in line with the usual distribution at our university. The mean age of the studied population is 22 years; and the median number of years of Internet use is 9—showing that their generation has been exposed to the Internet since their childhood. A detailed description of the sample is provided in Appendix A.

5. Results and discussion

In line with our expectation — and given the amount of exposure received by IT security — 91% of the students answered that security risks have increased in recent years, while only 4.5% thought risks stayed the same and 4,5% thought risks decreased. We conclude that the students feel there is an urgency about security matters, which leads to the next point: 94% of them stated that their attitude has changed towards being more careful regarding security matters. Only 6% stated that their attitude remained unchanged, and *none* said their attitude become more relaxed.

Next, we asked our respondents about their sources of information (allowing for multiple answers). 45% stated they learned at school, and 43% from other resources. Only 6% were instructed at work - because a small proportion of these undergraduate students currently hold regular jobs. Another 12% answered that they had no training at all - a fact that should be considered by the University. Looking at the academic curriculum of the Faculty of Accounting and Management Information Systems will conclude that, for the bachelors' programs, there is one compulsory course (accounting systems) that includes, indirectly - as a second focus, information security issues. This explains, partially, the students' responses

(45% stated they learned at school) and the insufficient training on information security issues. The academic curriculum, however, includes specific curses on the topic in most of the masters' programs.

In fact, when asked who they feel should be responsible for their information security training, the respondents agreed that the University should train them (99%), that employers are also responsible (100%), but that users should educate themselves, as well (90%). Thus we find there is considerable interest in learning about security. The students' responses indicate, correctly, the university's role in their training on the topic.

The majority of students (70%) think - correctly - that anti-virus software is not enough to protect them against security threats. This agrees with the fact that anti-virus software is increasingly less effective in safeguarding against attacks, and that hackers become more competent at evading security measures (Birtstone, 2015).

However, most of the respondents (88%) use anti-virus software as their main security defense, and 24% use the firewall built in their operating system. Only 67% answered that they update the operating system, which is unexpectedly low since updates can be done automatically and the lack of updates represent a major security threat (in a following question, 69% stated they run automatic updates). 36% of the respondents run backups, and 52% stated that they do not open e-mail attachments from unknown persons - implying that an important 48% do open such attachments, which represent a major attack vector.

A significant finding is that 85% of the students do *not* know what a phishing attack is (for example fake e-mails attempting to steal sensitive data). We think this is important because phishing attacks are increasing in frequency and impact, as on-line banking and on-line payments grow in number and volume. The current trend in contactless and mobile payments will yield new attack opportunities, as well (Leyden, 2014). This lack of information proved by the students is the result of the fact that these kinds of issues are included in the curriculum for the masters' programs.

Another important finding is that the majority of the students (58%) think that their computers are uninteresting for hackers. This leads to a false sense of security, as hackers are interested in *any* machine - to send spam, mine for crypto-currencies, comb the hard drive for data, encrypt data and ask for ransom (Cookson & Kuchler, 2014), and most importantly, intercept sensitive usernames and passwords, such as those used for on-line banking. 52% of the respondents think that if they format the hard drive, the data is completely deleted - which is false, and again creates a false sense of security. These two points in conjunction can lead to sensitive data being available for hackers.

However, the majority of the respondents (75%) think their computers are secured, which is in line with the percentage applying security updates (65%) and running an anti-virus (88%). Even if these measures are not enough, they represent an important starting point in security defense and awareness. We should also note that the remaining 25% feel their computers are unsafe.

Only 76% stated that they worry about data security in the context of banking transactions and on-line commerce, which is very low, but again in line with the rest of the answers. As instructors, we feel it is imperative that the students be exposed to the risks of on-line transactions - such as passing credit card data over unencrypted sites, or accessing a bank portal from a PC without security updates. The situation is made worse by the fact that 73% agree that they download music and movies using bit-torrent sites, which poses a major security threat due of the possibility of virus infection—besides the copyright issues. The users without updates and anti-virus are high-probability targets when downloading unsafe content from the Internet.

Perhaps the most surprising finding was that 74% of the respondents have had (or know someone who has had) problems with viruses or on-line account break-ins. This strongly contradicts the previous result, where 75% stated their computers are safe - and if that is true, then the percentage of respondents who have experienced problems should have been lower.

The students are not concerned about privacy; 93% stated they use social networks to share personal data with friends. We also attempted to evaluate students' opinion regarding the creation of user profiles on web sites, and only 31% stated they are concerned about the entity collecting the data, and 27% said they are worried about how their data will be used. We must note that the most prominent social networks explicitly state in their terms of service that collected data can be used with almost no restrictions by the sites collecting it (Facebook Data Policy, 2015).

Finally we asked the students about the operating systems they use, and 100% of them use Windows, 51% use Android and 6% use iOS—leading to the finding that 56% of the students use smartphones. This reflects the current trend in strong mobile growth, and should concern university instructors, as the smartphone becomes a more important business tool.

In H1 we posit that the students are aware of the current climate and raising importance of information security. Our poll evaluated on a Likert scale, from 1 to 5 whether information security issues have increased recently (with 1 corresponding to a decrease, 3 being neutral, and 5 representing an increase).

Using SPSS V24 we run a t-test with a hypothesized average of 3. The mean of the sample is 4.73 with standard deviation of .914, and the test concludes significantly (Sig. 2-tailed=0) that the students appreciate that information security issues have increased.

We tested whether the students' behavior has modified in response to the perceived security issues (Likert scale, 1=less strict attitude, 5=a lot more careful). The sample average was 4.33 with standard deviation σ=0.587, and the test was significant with Sig. 2-tailed=0. From these two tests, we conclude that H1 is validated and that students are aware of the current information security climate and have reacted by increasing their safeguards.

Table 1. Students' opinion on recent information security issues – t-test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
5. In recent years, do you appreciate that issues related to information security have:	15.501	66	.000	1.731	1.51	1.95

In H2 we posit that the students express a need for more training in information security. We formulated questions 8.1 through 8.3 on a Likert scale (1=not interested; 5=very interested) asking who should be responsible for the students' information security education (8.1—the school, 8.2—employers, 8.3—users themselves). All the questions yielded statistically significant positive answers, thus validating H2. We also asked whether the students are *not* interested in such a training (question 8.4), and whether InfoSec training is not required as long as there is anti-virus protection (8.5), and both questions received negative answers at a statistically significant level.

Table 2. Students' opinion on InfoSec Education – t-test

	Test Value = 3					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
8.1 The school should educate us	17.615	66	.000	1.299	1.15	1.45
8.2 The companies should instruct their employees	16.818	66	.000	1.269	1.12	1.42
8.3 Computer users should educate themselves	12.684	66	.000	1.239	1.04	1.43
8.4 I'm not interested in such a training	-7.628	66	.000	-1.000	-1.26	-.74
8.5 Training is not required as long as there is antivirus software	-7.600	66	.000	-.910	-1.15	-.67

To test H3 we ran an independent samples t-test and the result was statistically significant with Sig. 2-tailed = 0.408. Thus we accept H3, and we conclude that students who know about phishing attacks are less prone to security incidents, proving that training helps mitigate information security risks.

Table 3. Students' opinion on personal data sharing – t-test

	12. Do you know what a phishing attack is?	N	Mean	Std. Deviation	Std. Error Mean
19. You, or someone you know, has had computer-related security issues (viruses, e-mail or Facebook account hack etc)	0	57	1.65	.876	.116
	1	10	1.40	.843	.267

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
19. You, or someone you know, has had computer-related security issues (viruses, e-mail or Facebook account hack etc)	Equal variances assumed	1.507	.224	.834	65	.408	.249	.299	-.348	.846
	Equal variances not assumed			.857	12.658	.408	.249	.291	-.381	.879

H4 aimed to test whether students are care about privacy, and whether their stated opinion is supported by their actions. In a yes/no question (18.7) about whether they worry about the entity collecting their data, only 31% answered positive, leading to the conclusion that 69% are not concerned about such issues. An even smaller proportion is concerned about *how* their personal data is used. Moreover, question 15 asked whether the students use social networks to share data, and 93% of them do, yielding a statistically significant result. Thus we reject H4, concluding that the majority of the students know and do very little to protect their privacy.

Table 4. Students' opinion on personal data sharing – t-test

	Test Value = 0					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
15. I use social networks to share data with friends	28.608	66	.000	.925	.86	.99

In H5 we posit that the trust that students place in their information security skill is not supported by real-world actions. For this, we need to connect several questions together, and although there is no direct statistical relation between the results, we must use real-world judgment: 75% of the students feel their computers are properly secured. The result is statistically significant, meaning that there is strong evidence that the students believe their computers are secured.

Table 5. Students' opinion on personal computer security – t-test

	Test Value = 1					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
16. How secured is your computer?	20.578	66	.000	1.224	1.11	1.34

However, the opinion stated above is at odds with the following:

- Only 25% of the students run a firewall;
- 52% of the students (wrongly) believe that all data will be deleted from a formatted hard drive;
- 58% of them (wrongly) believe that their computers are uninteresting for hackers;
- 85% do not know what a phishing attack is (and 48% would open attachments from unknown sources).

Based on industry best practices, we judge that there is a discrepancy between the student's perceived level of security and the real-world actions. As the students gradually get enrolled in the workforce, they will carry on their practices and opinions, thus extending the risks onto their employers. But this gap can certainly be addressed by training (for which there is support, as per H2).

6. Conclusions

The need for a real awareness, robust solutions and training in regard with information security is dramatically proved by the security breaches registered every year in all industries and companies no matter their size. In this respect the students have to be trained in regard with this important issue. This is imposed by the new professional requirements demanding solid IT knowledge and the IT environment existing in any company.

The accounting profession is facing with high requirements arising from the IT field. The accountant is performing his work in a digital environment demanding IT skills and expertise. The entire accounting process and its control are adjusted to the new requirements and constraints imposed by the software (Stanciu & Bran, 2015). No matter the domain the accountant is performing its work the IT issues are present. Working in a digital ecosystem the accountant professional has to understand the cyber risks induced by this environment and react properly. In this respect, the universities' curriculum has to include more time allocated to information security starting with bachelors' programs and continuing with masters' programs. The curriculum expand on information security issues does not exclude specific trainings organized by the university, starting with the first year students (taking into consideration the need to be informed in regard with the information security policy of the university and the main procedures regarding IT platforms and other IT resources they'll use).

We conclude that students might have a certain technical knowledge but this is not enough in respect with information security requirements, given the current climate. They need a more training towards risk awareness approach and behavior. Dedicated programs for information security awareness are also a solution for the students' training. Even with the current limitation of the budges and resources the universities should develop such programs, in e-learning approach, for all the students, but mostly for the first year students. The monitor of the students' awareness regarding information security is recommended and the students enrolment in new trainings if necessary.

References

Dimensional Research (2011) "The Risk of Social Engineering on Information Security: A Survey of IT Professional", available on-line at http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf

Birtstone, R (2015) "Don't count on antivirus software alone to keep your data safe", available on-line at http://www.theregister.co.uk/2015/02/09/dont_ count_on _antivirus_alone_to _protect_your_data/

CISCO (2014) "Cisco 2104 Annual Security Report", available on-line at http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html

Cooldige, M. (2015) "Netskope report reveals high frequency of compromised credentials in enterprise cloud apps", available on-line at http://www.prnewswire.com/news-releases/netskope-report-reveals-high-frequency-of-compromised-credentials-in-enterprise-cloud-apps-300017649.html

Drtil, J. (2013) "Impact of information security incidents – theory and reality", *Journal of Systems Integration*, no.1: 44-52

Dunsmuir, L. & Finkle, J. (2015) "U.S. Charges three in ring that stole 1 billion email addresses", Reuters, available on-line at http://www.reuters.com/ article/2015/03/06/usa-cybercrime-justice-idUSL1N0W81QY20150306

EY (2014) "Get ahead of cybercrime", EY's Global Information Security Survey, 2014, available on-line at http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

Eyon, K. (2013) "information security awareness of business college: undergraduate student", *Information Security Journal: A Global Perspective*, available on-line: 18 Nov 2013

Eyong, K. (2014) "Recommendations for information security awareness training for college students", *Information Management and Computing Security*, vol. 22(1): 115-126

Goodman, K. (2015) "Future crimes: A journey to the dark side of technology – and how to survive it", Random House, LLC, New York: 10-12

Facebook Data Policy, available on-line at "https://www.facebook.com/ about/privacy/"

ISO/IEC 27001 "Information technology – Security techniques – Information Security Management Systems – Requirements" ISO/IEC 27001:2005, International Organization for Standardization and International Electrotechnical Commission

ISO/IEC 27002:2005 "Information technology – Security techniques – Code of practice for information security management" ISO/IEC 27002:2005. International Organization for Standardization and International Electrotechnical Commission

Kookson, R. & Kuchler, H. (2014) "NCA and FBI disrupt global malware network", *Financial Times*, available on-line at http://www.ft.com/intl/ cms/s/0/495f720c-ea77-11e3-8dde-00144feabdc0.html#axzz3UcO0wZJm

Leyden, J. (2014) "Apple Pay a haven for 'rampant' credit card fraud, say experts", available on-line at http://www.theregister.co.uk/2015/03/03/apple_pay_ plastic_fraud/

Leyden, J. (2014) "FBI warns of disk nuke malware after Sony Pictures megahack", available on-line at http://www.theregister.co.uk/2014/12/02/ malware_warning_follows_ sony_megahack

Leyden, L. (2015) "NSA, GCHQ ransacked SIM maker Gemalto takes a $500m stock hit", available on-line at http://www.theregister.co.uk/ 2015/02/20/gemalto_sim_surveillance _fallout/

OECD (2002) "OECD guidelines for the security of information systems and networks: Towards a culture of security", OECD Publications, Paris, France: available on-line http://www.oecd.org/sti/ ieconomy/15582260.pdf

NIST (1998) "NIST SP 800-16 Information Technology Security Training Requirements: A role – and Performance – Based Model", available on-line at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

PWC (2013) "Changing the game. Key findings from the global state of information security survey 2013", available on-line at http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

PWC (2014) "2014 Information Security Breaches Survey. Technical report", Department of Business innovation and skills UK PWC, available on-line at http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

Rastogi, R. & Solms, von R. (2012) "Information security service branding – beyond information security awareness", *Systemics, Cybernetics and Informatics*, vol. 10 (6): 54-55

Sanger, D. & Perlroth, N. (2015) "Bank hackers steal millions via malware", *The New York Times*, available on-line at http://www.nytimes.com/2015/02/15/ world/bank-hackers-steal-millions-via-malware.html?_r=0

Stanciu, V. & Bran, F.P. (2015) "The accounting profession in the digital era", *Quality - Access to Success Journal. Proceedings of the Ecological Performance in a Competitive Economy*, vol. 16, S1: 546-551

APPENDIX A – Sample characteristics

Measure	Categories	Freq.	%	Cum.
Security incidents have	Increased	61	91%	91%
	Remained Constant	3	4.5%	95%
	Decreased	3	4.5%	100%
Attitude towards security	A lot more careful	26	39%	39%
	More careful	37	55%	94%
	Unchanged	4	6%	100%
	Less strict	0	0%	100%
	A lot less strict	0	0%	100%
Where have you learned about information security (multiple)	At work	4	6%	
	At university	30	45%	
	Self-study	4	6%	
	Others	29	43%	
	Nobody told me	8	12%	
The school should educate us	Strongly disagree	0	0%	0%
	Disagree	1	1%	1%
	Neutral	2	3%	4%
	Somewhat agree	40	60%	64%
	Strongly agree	24	36%	100%
The companies should instruct their employees	Strongly disagree	0	0%	0%
	Disagree	0	0%	0%
	Neutral	6	9%	9%
	Somewhat agree	37	55%	64%
	Strongly agree	24	36%	100%
Users should educate themselves	Strongly disagree	1	1%	1%
	Disagree	0	0%	1%
	Neutral	9	13%	14%
	Somewhat agree	29	43%	57%
	Strongly agree	28	42%	100%
I'm not interested in such a training	Strongly disagree	27	40%	40%
	Disagree	22	33%	73%
	Neutral	11	16%	89%
	Somewhat agree	5	7%	96%
	Strongly agree	2	3%	100%

Measure	Categories	Freq.	%	Cum.
Training is not required as long as there is anti-virus software	Strongly disagree	21	31%	31%
	Disagree	26	39%	70%
	Neutral	14	21%	91%
	Somewhat agree	5	7%	98%
	Strongly agree	1	1%	100%
Security for your home computer (multiple)	Anti-virus	59	88%	
	Anti-virus from service provider	2	3%	
	Anti-spyware	7	10%	
	Anti-spam	5	7%	
	Firewall within anti-virus or OS	16	24%	
	Firewall (self-installed)	5	7%	
	None of the above	2	3%	
	I'm not aware if I have any	1	1%	
	I update OS and browser	45	67%	
	I run backups	24	36%	
	I don't open unknown attachments	35	52%	
	Users have different accounts	3	4%	
	Periodically change e-mail address	2	3%	
	Encrypt important files	5	7%	
	Connect to Interned only when necessary	4	6%	
Does your computer run automatic updates?	Yes	46	69%	69%
	No	21	31%	100%
Do you know what a phishing attack is?	Yes	10	15%	15%
	No	57	85%	100%
If you format your hard drive, data is completely deleted	True	35	52%	52%
	False	32	48%	100%
My computer is uninteresting for hackers	True	39	58%	58%
	False	28	42%	100%
I use social networks to share data with friends	True	62	93%	93%
	False	5	7%	100%

Measure	Categories	Freq.	%	Cum.
How secured is your computer?	Very secured	2	3%	3%
	Secured	48	72%	75%
	Unsecured	17	25%	100%
How concerned are you about InfoSec regarding on-line banking and purchases?	Not concerned	7	10%	10%
	Somewhat concerned	9	13%	23%
	Concerned	31	46%	70%
	Very concerned	19	28%	98%
	I should be but I am not	1	1%	100%
The reason I do not sign-up with sites	Takes too long	13	19%	19%
	Requires name	2	3%	22%
	Requires e-mail	2	3%	25%
	Requires postal address	2	3%	28%
	Doesn't say how data will be used	18	27%	55%
	Not worth	8	12%	67%
	I don't trust the entity collecting the data	21	31%	99%
	I always complete a profile	1	1%	100%
You, or someone you know, has had computer security problems	True	43	64%	64%
	Somewhat true	10	10%	75%
	False	25	25%	100%
I download music and movies from torrent sites	True	42	63%	63%
	Somewhat true	9	13%	75%
	False	16	24%	100%
I use my University on-line account to fin out exam scores and other data	True	67	100%	100%
	False	0	0%	100%
What OS do you use (multiple)	Windows	67	100%	
	OSX	0	0%	
	Linux	1	1%	
	Android	34	51%	
	iOS	4	6%	