South African Computing Educators' Perspectives on Information Security Behaviour

Thandolwethu Mabece, Lynn Futcher, Kerry-Lynn Thomson

South African Computing Educators' Perspectives on Information Security Behaviour

Thandolwethu Mabece[1], Lynn Futcher[2] and Kerry-Lynn Thomson[3]

[1,2,3] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
{s213258919@nmmu.ac.za, Lynn.Futcher@nmmu.ac.za,
Kerry-Lynn.Thomson@nmmu.ac.za }

Abstract. With the growing dependency of users on computers, technology and the internet, the protection of information and information systems is of utmost importance. Current computing graduates will become tomorrow's users and protectors of information and information systems. It is, therefore, essential that higher education institutions provide adequate information security education to enable these graduates to protect information and related information systems. This information security education should, preferably, be a part of their formalized studies. This paper discusses the opinions and experiences of computing educators regarding the extent to which information security is currently integrated within computing curricula and the current information security behaviour of computing students and educators. A total of twenty educators, from six South African higher education institutions, all universities, voluntarily participated in this study. Results indicated that there was limited information security integration within computing curricula at these higher education institutions. This could potentially negatively impact the information security behaviour of computing graduates. However, since behaviour is complex in nature, this paper briefly suggests various factors that could positively influence the information security behaviour of computing students and should be taken into consideration by computing educators.

Keywords: Information security education, information security behaviour, computing curricula, computing students, pervasive information security

1 Introduction

User behaviour accounts for the majority of security breaches experienced by organisations, although often not with malicious intent to cause harm [1,2]. Users who have not been educated with regard to information security could be easy targets for hackers because of their ignorance. Therefore, educated and trained users could be a critical success factor in order to mitigate threats within organisations [3,4]. Once computing graduates leave higher education institutions, many become employees within organisations with various responsibilities including; designing and developing software, maintaining networks and information systems. Computing in this context

refers to Computer Science (CS), Information Systems (IS) and Information Technology (IT).

Various Association for Computing Machinery (ACM) curricula guidelines [5,6,7] describe what characteristics computing graduates should have once they have completed their degrees. The ACM CS guidelines [5] explain that a graduate "*needs a set of general principles, such as sharing a common resource, **security**, and concurrency*. The ACM IS guidelines [7] refer to Information Assurance and Security (IAS) as IT security and risk management. The ACM IT guidelines [6] specifically state that an IT graduate should have an "*understanding of professional, ethical, legal, **security** and social issues and responsibilities*". Furthermore, the IT guidelines [6] describe IAS as an integrative knowledge area that should be pervasive throughout other knowledge areas. Pervasive, in this context, is defined as "*existing in all parts of a place or thing; spreading gradually to affect all parts of a place or thing*" [8]. In order for information security to be pervasively integrated into a computing curriculum, it must be formally planned and integrated across various modules within each knowledge area. The CS, IT and IS computing guidelines [5,6,7] suggest that graduates from these disciplines should be conscious of information security, particularly when they become employed within organisations. It is important that they stay abreast of industry trends, as these graduates need to be able to solve current real world problems. If the curriculum does not offer the necessary tools needed to solve these real world problems, then the higher education institution has failed [6].

Education is often the only way to convince users of the need to do things differently [9]. Schneider [10] argues that an educated workforce is essential to building trustworthy systems. In the same way, computing graduates who are conscious of information security could design and build systems that protect information. According to Schein [9], people will often refuse to accept the need for new, responsible behaviour patterns until they have acquired the relevant information security knowledge, skills and insight.

According to Hu et al [11], information security culture shapes and guides information security behaviour. Similarly, an organisation's information security culture is cultivated by the information security behaviour of its employees [12]. If an information security culture does not exist within an organisation, the behaviour of new employees, for example computing graduates, coming into the organisation could influence the cultivation of an information security conscious culture [13,14]. As information security threats continue to be a grave concern, the importance of information security education cannot be stressed enough in computing curricula [15].

In terms of this paper, it is important to determine the perspectives of computing educators with regard to information security education and behaviour. Section 2 discusses information security behaviour, while Section 3 explains the purpose of this study. Section 4 describes how this research was conducted including the interview process, participants and the structure of the questionnaire. Section 5 highlights the results and findings, while Section 6 provides a discussion of the survey results. Section 7 briefly suggests various factors that could possibly influence the information security behaviour of students, while Section 8 concludes the paper.

2 Information Security Behaviour

Information security is not solely a problem of technology, but more often than not, it is a human problem. The greatest threat to information security could be employees who are not information security conscious [16,17]. Information security behaviour refers to the behaviour of employees when they engage with information systems, including hardware, software and network systems. Such security-related behaviours have major implications for information security [18]. Depending on its nature, employee behaviour may either pose a risk or reduce threats to information assets. Information security behaviour is classified into four broad categories, according to Guo [18]. These categories include security assurance behaviour, security compliant behaviour, security risk-taking behaviour and security damaging behaviour.

Security Assurance Behaviour (SAB): SAB refers to intentional behaviours that employees carry out actively to protect information assets and information systems. In other words, this behaviour refers to employees that are information security conscious. This is the most desirable behaviour from an information security management perspective. Examples of SAB include identifying and being aware of threats and implementing the necessary security measures to counteract those threats. A significant characteristic of SAB is that it implies conscientious action, which means that employees make an effort to behave securely [18].

Security Compliant Behaviour (SCB): SCB refers to intentional or unintentional behaviours that adhere to organisational information security policies. According to Guo [19], SCB may be intentional in that employees make a conscious effort to avoid infringing security policies. It may also be unintentional in that employees may do something without thinking about security issues in mind, although their behaviour might still be adhering to security policies. Employees in the SCB group can be viewed as doing what they are required to do [18].

Security Risk-taking Behaviour (SRB): SRB refers to intentional behaviours that may put information systems at risk, although not with the intentional motive to cause damage. In other words, employees may put organisations at risk unintentionally by, for example, writing down passwords, leaving sensitive documents lying around or visiting websites that are not secure. This behaviour can be likened to that of a non-malicious security violation [20]. Employees in this group are not doing what they are supposed to do [18].

Security Damaging Behaviour (SDB): SDB refers to intentionally damaging behaviours that can cause significant damage to information systems. These behaviours are malicious and deliberate, and can be subject to punishment under the laws and regulations of the society rather than policies [18]. Examples of SDB include industrial espionage, fraud and information theft. Essentially, employees that are categorised in this group are intentionally doing what they are prohibited from doing.

Based on this discussion regarding the different security-related behaviours, it is evident that SAB is the ideal behaviour to ensure information security. When computing students graduate from higher education institutions, they are likely to be employed by organisations. As such, they will be expected to protect organisational information systems and related information assets. Therefore, they need to be

educated on how to provide the required protection. Ideally, this should be done before graduating. Higher education institutions are responsible for producing computing graduates who are information security conscious and who meet industry needs with regards to information security [21].

Computing students who have not been educated with regards to information security could typically fall into the SRB category. This is mainly due to the fact that they may not be aware that their actions or inactions, pose a risk to information assets and information systems. The ideal situation would be one where computing students demonstrate SAB before graduating and becoming employees. Over time, information security education could lead to an information security culture where the normal behaviour is SAB.

3 Purpose of the Study

It is currently not known to what extent information security is integrated into undergraduate computing curricula in South African higher education institutions. In addition, the information security behaviour demonstrated by computing students and educators is unknown. The purpose of this study was, therefore, to address two main objectives. The first objective was to determine the perspectives of computing educators regarding the extent to which information security is currently integrated into computing curricula. The second objective was to determine the current information security behaviour of computing students and educators as perceived by computing educators. In order to meet these objectives, this study gathered opinions and experiences from computing educators at six South African higher education institutions. In addition, this paper suggests various factors that could influence the information security behaviour of computing students.

4 Research Process

This section explains the process that was followed in order to collect data from the participants. It must be noted that this is an initial study to gather the perspectives of computing educators with regard to information security education and behaviour. These computing educators were from the CS, IS and IT disciplines to gather a general perspective. However, the purpose was not to do a comparative study across these disciplines. In addition, this section describes the semi-structured interview process, the participants, as well as the design of the questionnaire that was used as a basis for the interviews conducted. This study used a mixed method approach, including both quantitative and qualitative data.

Interview Process: A semi-structured interview was conducted with twenty participants with the aid of a questionnaire to gather the opinions of the participants. Participation in this study was voluntary and participants remain anonymous.

Participants: The participants were selected from six South African higher education institutions, all universities. Three were from CS, eight from IT and nine from IS.

Questionnaire Design: The questionnaire was divided into two sections with each section focusing on a single objective. The primary aim of Section 1 was to ascertain the opinions of the participants on whether information security was currently integrated within their undergraduate computing curriculum and their general views on the pervasive integration of information security. The purpose of Section 2 was to determine the opinions and observations of participants with regard to the information security behaviour of their students, as well as their colleagues. Sections 1 and 2 consisted of closed (yes/no) and open-ended questions thereby gathering both quantitative and qualitative data. The following section provides the results and findings of this initial study.

5 Results and Findings

The purpose of this section is to provide the results and findings of the semi-structured interviews based on the questionnaire briefly described in the previous section.

Section 1 - To determine computing educators' perspectives regarding the extent to which information security is currently integrated within computing curricula: Table 1 represents the number of participants who answered "yes" or "no" to the closed questions for the first objective. It is important to note that the table does not show the complete list of questions for this section, as some were open-ended questions. However, answers to both the closed and open-ended questions are discussed in this section.

Table 1: Section 1 Closed Questions and Responses

Section 1 Closed Questions		Yes	No
1.1	Do you teach any security-related modules?	9 (45%)	11 (55%)
1.3	Is information security pervasively integrated within other modules?	14 (70%)	6 (30%)
1.5	Do you think information security should be an important part of your discipline?	19 (95%)	1 (5%)
1.8	Do you think that your colleagues share the same views with regards to pervasively integrating information security?	19 (95%)	1 (5%)
1.10	Do you foresee any perceived challenges with regards to pervasively integrating information security?	18 (90%)	2 (10%)

As shown in Table 1, 11 (55%) of the participants indicated that they did not teach any specific security-related modules (Question 1.1). In response to Question 1.2, the 9 (45%) participants who answered "yes" to Question 1.1 indicated they taught security-related modules ranging from 1st year through to the 5th year of study.

For Question 1.3, it must be noted that even though the question asked if information security was pervasively integrated, on further enquiry most participants

misinterpreted the term *pervasive*, as they perceived the ad hoc discussion of information security concepts in some modules as being pervasive. For example, 14 (70%) of the participants indicated that there are certain modules that include a few aspects of information security (Question 1.3). Therefore, these participants misinterpreted this as being pervasive. Examples of the modules where information security aspects were mentioned include: project management, databases, application development and forensics (Question 1.4). 19 (95%) of the participants agreed that information security should be an important part of their discipline (Question 1.5). In response to Question 1.6, one participant indicated that people interact with information and information systems on a daily basis; thus they should be able to protect those information systems. Other participants indicated that it is important for everyday life as information security is a real world problem. The participants' perceptions on the pervasive integration of information security is that it is important to integrate information security. However, many participants mentioned that it should be contextualised within the applicable modules (Question 1.7).

19 (95%) participants indicated that they thought their colleagues shared the same views as they did with regard to pervasively integrating information security (Question 1.8). Others indicated that only those colleagues with some information security background knowledge shared the same views with regard to the integration of information security (Question 1.9). However, 18 (90%) of the participants indicated that they foresaw challenges with regard to the pervasively integration of information security into their modules. In answer to the open-ended Question 1.11, some of the perceived challenges they foresaw included: not enough time within their existing modules to include information security; information security is too technical; and educators do not know *how* to integrate information security within their respective modules. These were the predominant challenges indicated by participants.

Section 2 - To determine the current information security behaviour of computing students and educators as perceived by computing educators: Table 2 represents the number of participants who answered "yes"' or "no" for each closed question.

Table 2: Section 2 Closed Questions and Responses

	Section 2 Closed Questions	Yes	No
2.1	Do you think that your students behave in a secure manner?	6 (30%)	14 (70%)
2.3	Are you aware of any information security behavioural policies within your institution?	0 (0%)	20 (100%)
2.4	Are students aware of any ICT-related policies?	9 (45%)	11 (55%)
2.5	Are there any consequences for "insecure" behaviour?	17 (85%)	3 (15%)
2.7	Does an information security culture exist in your department amongst colleagues?	14 (70%)	6 (30%)

As can be seen in Table 2, 14 (70%) of the participants indicated that their students do not behave securely (Question 2.1). In relation to Question 2.2, examples provided by the participants indicated that their students did not behave in a secure manner as they tend to share passwords and accounts. They also do not log off their computers and they do not scan their USB sticks.

All of the participants (100%) indicated that they were not aware of any specific information security behavioural policies that exist at their respective institutions. Upon further investigation, participants mentioned that their higher education institutions had ICT usage policies that students had to comply with (Question 2.3). 9 (45%) of the participants indicated that their students were aware of the ICT usage policies (Question 2.4). Furthermore, 17 (85%) of the participants indicated that there were consequences for "insecure" ICT usage policy behaviour (Question 2.5). Consequences provided by participants for "insecure" ICT usage behaviour (Question 2.6) include: disciplinary hearings; disabling accounts; community service; and banning students from computer laboratories.

14 (70%) of the participants specified that an information security culture does exist within their department amongst colleagues (Question 2.7). However, it was indicated by participants that the security culture that does exist within their department seems to be limited to locking office doors, protecting examination papers with passwords when sent via email and logging off unattended computers (Question 2.8).

Some examples highlighted by participants with regards to how they would influence students and colleagues to behave more securely included (Question 2.9): increased information security knowledge, education and awareness; contextualised information security examples; information security scenarios and scare tactics.

6 Discussion

The various ACM computing curricula guidelines [5,6,7] clearly present IAS as an integrative knowledge area that should permeate other knowledge areas. However, results from the survey show that there is limited information security integration within the computing curricula of the universities surveyed. The possible reason for the limited integration could be the challenges as perceived by computing educators. Participants indicated that possible challenges for pervasive integration could be that educators did not know how to integrate security; they do not have enough time within their modules; and that information security is too complex. More focus should be placed on ways to incorporate information security practically within these modules so that it permeates throughout the curriculum. There needs to be a conscious effort from computing educators in this regard.

Participants generally acknowledged the importance of information security as being an integral part of any ICT practitioner's daily life. The participants from the IS discipline in particular emphasised that information was at the core of what they did within their discipline.

The majority of the participants were willing to consider the integration of information security into their modules. The participants indicated that they would

prefer small, contextualised information security examples that are applicable to each of their specific modules. In addition, many indicated that they were not equipped with any guidelines on *how* to integrate information security concepts into their modules. This poses a great challenge since the ACM states that information security should be a pervasive theme, but they do not suggest ways in which this can be done.

The majority of participants indicated that their students did not act in a secure manner, since they shared accounts and passwords, remained logged onto their computers when unattended and did not scan USB sticks. This result suggests that the behaviour of many students falls into the SRB category and that there is a significant need for change in their information security behaviour.

Most of the participants indicated that a limited information security culture existed within their work environment amongst colleagues. If an information security culture does not exist within computing departments, it is possible that computing students will not act in a secure manner.

As discussed in Section 2, intentional SAB is the desired information security behaviour that computing graduates should demonstrate. It cannot, however, be expected that SAB will evolve naturally. There should be a conscious effort by computing educators to integrate information security into their modules, which could positively influence the conscientious behaviour of computing graduates. However, from this study, it can be concluded that many computing educators in South Africa are not *consciously* doing enough to positively influence the information security behaviour of their computing graduates. In order to address this, future research could be conducted to help educators consider the various factors that could influence the information security behaviour of their students. The following section suggests possible factors to be considered in future research.

7 Factors Influencing Information Security Behaviour

Many behavioural theories exist in an attempt to explain why humans behave the way they do. Each theory focuses on different factors in order to explain the behaviour of people. While many behavioural theories exist, the theories briefly referred to in this paper include the Theory of Planned Behaviour, Protection Motivation Theory and the Social Cognitive Theory.

The **Theory of Planned Behaviour** explains the links between various concepts that could influence behaviour. As the name suggests, this theory helps to predict the deliberate behaviour of people because behaviour can be planned [22]. The Theory of Planned Behaviour has been widely used in investigating ethical behaviours when using information systems and the decisions of individuals to adopt acceptable computer or information security measures [23]. According to this theory, attitude, subjective norms and perceived behavioural control all influence a person's intention, which ultimately could determine their behaviour.

The **Protection Motivation Theory** is considered to be one of the leading theories in the area of health behaviour motivation. However, it has been extended to various other fields of research. It is widely used as an explanatory theory to predict

individual intentions to take precautionary or protective measures when faced with threats [24,25,26].

The **Social Cognitive Theory** explains how people acquire and maintain certain behavioural patterns. According to the theory, evaluating behavioural change depends on personal factors, behavioural factors and environmental factors [27].

In order for computing students to demonstrate the desired security assurance behaviour (SAB), factors that could influence such behaviour need to be addressed. Table 3 indicates some factors from the above-mentioned theories that could influence the behaviour of computing students.

Table 3: Factors that could influence information security behaviour

Influence	Factor	Theory
Personal and Behavioural	Attitude	Theory of Planned Behaviour
	Perceived behavioural control and self-efficacy	Theory of Planned Behaviour Protection Motivation Theory
	Perceived vulnerability and perceived severity	Protection Motivation Theory
	Outcome expectancy	Social Cognitive Theory
Environ-mental	Subjective norms, Modelling, Identification and Culture	Theory of Planned Behaviour Social Cognitive Theory Social Cognitive Theory

Attitude - computing students with a positive attitude towards information security are more likely to adhere to the required SAB, while those with a negative attitude are less likely to adhere to the required SAB.

Perceived behavioural control and self-efficacy - computing students with a high perceived behavioural control and self-efficacy are more likely to execute the required behaviour as opposed to computing students with a low perceived capability. When it comes to information security and the protection of information assets, it is important for computing students to have high perceived behavioural control and self-efficacy so that they could demonstrate the desired SAB.

Perceived vulnerability and perceived severity - computing students should be educated about the various threats that they are susceptible to in order for them to protect themselves from those threats. If computing students do not know that they are susceptible to information security threats, they are less likely to behave in a secure manner with regard to information assets and information systems. In addition, computing students should be aware of the potential impact that information security threats can have on information assets and information systems.

Outcome expectancy - if computing students do not adhere to an ICT usage policy in laboratories, they could be denied access. Therefore, the outcome expectancy of the computing students would be that if they do not adhere to the ICT usage policy, they

would be denied laboratory and internet access. This negative consequence could influence computing students to demonstrate SAB.

Subjective Norms, Modelling, Identification and Culture - it is important that higher education institutions have a positive information security culture. The information security culture could be influenced by subjective norms, modelling and identification – all of which are ways in which people learn through social pressure and observation. Furthermore, it is important that higher education institutions provide computing students with an environment where SAB is the norm. It could be argued that if computing students have role models they can identify with, for example their educators, they too could be influenced to display the desired SAB.

Further considerations, not directly linked to behavioural theories, include policies and education.

Policies - information security policies are important within organisations as they dictate the appropriate behaviour of employees [28,29]. Similarly, an information security policy within higher education institutions should provide guidance to computing students on how to behave with regard to information security.

Education - information security education is important as it could provide computing graduates with the necessary knowledge, insight and skills they need to protect information assets within organisations. As discussed, the ACM specifically states that information security should be an integrative knowledge area that should permeate other knowledge areas.

Acceptable information security behaviour combined with technological and physical security measures could help to protect organisations effectively against malicious attacks [23,30]. In the same way that organisations should focus on the information security behaviour of their employees, higher education institutions should focus on influencing the information security behaviour of computing students.

8 Conclusion

In order to adequately protect the information assets of an organisation, it is important for computing students to acquire the necessary information security knowledge through education. The results from the semi-structured interviews suggest that participants generally accepted that information security is an important part of everyday life and thus should be taught in computing curricula. However, there is limited conscious effort from some computing educators to do this. It is believed that if computing students were exposed to information security through formal planning and integration across the curriculum, this could positively influence the information security behaviour of these students. However, for this to be effective, various factors need to be taken into consideration, as suggested in this paper.

Acknowledgements. The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

1. Tajuddin, S., Olphert, W., & Doherty, N. F. Relationship between stakeholders' information value perception and information security behaviour. In AIP Conference Proceedings (2014).
2. Tu, Z., & Yuan, Y. Critical success factors analysis on effective information security management : A literature review. Information Systems Security, Assurance, and Privacy Track (SIGSEC), 1–13 (2014).
3. Al Awawdeh, S. & Tubaishat, A. An information security awareness program to address common security concerns in IT unit. ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations (2014).
4. Cox, J. Information systems user security: A structured model of the knowing-doing gap. Computers in Human Behavior, 28(5) (2012).
5. ACM. Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (2013).
6. Lunt, B.M., Ekstrom, J. J., & Lawson, E. Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (2008).
7. Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Sipior, J. C., & de Vreede, G. J. IS 2010: Curriculum guidelines for undergraduate degree programs in Information Systems (2010).
8. Oxford Dictionaries. Oxford Dictionaries- Language matters. Oxford online dictionary. Available at: http://www.oxforddictionaries.com/definition/learner/pervasive [Accessed December 1, 2016] (2015).
9. Schein, E.H. The corporate culture survival guide: Sense and nonsense about culture change., San Francisco, CA: Calif.:Jossey-Bass (1999).
10. Schneider, F.B. Cybersecurity education in universities. IEEE Security and Privacy, 11 (2013).
11. Hu, Q., Dinev, T., Hart, P., & Cooke, D. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4) (2012).
12. Da Veiga, A. & Eloff, J.H.P. A framework and assessment instrument for information security culture. Computers & Security, 29(2) (2010).
13. Van Niekerk, J. & Von Solms, R. A holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (2005).
14. Von Solms, R. & Von Solms, B. From policies to culture. Computers & Security, 23 (2004).
15. Yoon, C., Hwang, J.-W. & Kim, R. Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education, 23(4) (2012).
16. Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. Analysis of personal information security behavior and awareness. Computers & Security, 56 (2015).

17. Shropshire, J., Warkentin, M., & Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Quaternary Geochronology, 49, 177–191. http://doi.org/10.1016/j.cose.2015.01.002 (2015).
18. Guo, K. H. Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32(1) (2013).
19. Guo, K. H. Revisiting the human factor in organizational information security management. ISACA Journal, 6 (2013).
20. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 203–236. http://doi.org/10.2753/MIS0742-1222280208 (2011).
21. Talib, M. A., Khelifi, A., & Ugurlu, T. Using ISO 27001 in teaching information security. In IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, Montreal, QC: IEEE. http://doi.org/10.1109/IECON.2012.6389395, (2012).
22. Ajzen, I. The Theory of Planned Behavior. Orgnizational Behavior and Human Decision Processes, 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T (1991).
23. Ifinedo, P. Understanding information systems security policy compliance: An integration of the Theory of Planned Behavior and the Protection Motivation Theory. Computers and Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007 (2012).
24. Safa, N. S., & Von Solms, R. An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442–451. https://doi.org/10.1016/j.chb.2015.12.037 (2016).
25. Siponen, M., Adam Mahmood, M., & Pahnila, S. Employees' adherence to information security policies: An exploratory field study. Information and Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006 (2014).
26. Yoon, C., Hwang, J.-W., & Kim, R. Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education, 23(4), 407–416. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84880826819&partnerID=40&md5=4a3c2d7fe56348029208741e54be814c (2012).
27. Bandura, A. Organisational applications of Social Cognitive Theory. Australian Journal of Management, 13(2), 275–302 (1988).
28. Höne, K., & Eloff, J. H. P. What makes an effective information security policy? Network Security, 14–16. https://doi.org/10.1016/S1353-4858(02)06011-7 (2002).
29. Von Solms, R., & Von Solms, B. From policies to culture. Computers and Security, 23, 275–279. https://doi.org/10.1016/j.cose.2004.01.013 (2004).
30. Furnell, S., & Clarke, N. Power to the people? the evolving recognition of human aspects of security. Computers and Security, 31(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004 (2012).