The Feasibility of Raising Information Security Awareness in an Academic Environment Using SNA

Rudi Serfontein, Lynette Drevin(✉), and Hennie Kruger

North-West University, Potchefstroom, South Africa
{rudi.serfontein, lynette.drevin, hennie.kruger}@nwu.ac.za

Abstract. The human aspect is one of the key success factors in information security (InfoSec). Its impact on InfoSec is so significant that multiple studies have shown that a balanced approach combining technology and security awareness is needed in order to maintain the integrity of an organisation's security. At present, one of the methods most often used to address InfoSec awareness is to develop security awareness programmes that can be used to educate its users within an organisation. This method has several drawbacks; however, as such programmes might not be comprehensive enough, or quick enough to address newer threats. It can furthermore lead to the users developing InfoSec fatigue, which renders most attempts at improving security awareness pointless. These problems are compounded by non-traditional organisational structures, such as those found in educational institutions, where both students and staff should be made aware of information security risks on a regular basis. In order to address the potential information security awareness problem at educational institutions, this paper investigates the feasibility of using Social Network Analysis (SNA) to improve existing security awareness programmes. Following a brief introduction to SNA, two illustrative examples are offered to show that SNA presents a viable option to improve programmes for raising information security awareness in an academic environment, by allowing for the effective selection of ideal target locations.

Keywords: Social network analysis · Security awareness · Security fatigue

1 Introduction

In the field of information security, one of the primary success factors is the human aspect [1]. Past research has shown that a balanced approach in which both technological and social aspects are addressed is crucial to maintaining information security [2–4]. Despite repeated campaigns to educate users regarding information security, however, a significant number of users still engage in risky online behaviour [5] and are still considered the weakest link in information security [6]. Among the many places that can be negatively impacted by a lack of information security awareness, few are as vulnerable as universities. This stems from the fact that university networks need to be accessible to a wide variety of people, such as students, faculty members,

L. Drevin and M. Theocharidou (Eds.): WISE 2018, IFIP AICT 531, pp. 69–80, 2018.
https://doi.org/10.1007/978-3-319-99734-6_6

administrative staff, and visitors [4]. With the massive number and types of people that need to be able to access a university network, it is only reasonable to assume that a significant number of users will act in a way that compromises both the security of the university and their own personal security. One of the best known traditional methods of addressing this risk and educating users is security awareness programmes [7–9]. There are, however, a number of significant drawbacks to these awareness programmes, e.g. the awareness programmes might not be comprehensive enough [10], they might not address new threats quickly enough when the risks change continuously [11], and the programmes rely upon the users to consciously decide to comply with information security principles [12]. A significant amount of research is focused on attempting to address these shortcomings [13]. Another factor that may impact negatively on security awareness training is security fatigue. Security fatigue is a specific form of mental fatigue, which is a well-known phenomenon in psychology that describes the feeling a person has during or after prolonged periods of cognitive activity [14, 15]. Security fatigue is experienced by users when they are bombarded with information security knowledge to such a degree that they become overburdened with the information and may choose to abandon all conscious efforts to adhere to the security principles as explained during the course of the awareness programmes [16].

Given the importance of the human aspect in information security and the potential problems with broad security awareness programmes, an adaptive approach is proposed. In this paper, the feasibility of using Social Network Analysis (SNA) as a technique to positively influence information security awareness programmes, specifically those that are targeted at an academic environment, will be discussed. SNA is a method used to graphically represent a social organisation, such as a community or business, in such a way that the social interactions can be studied quantitatively [17]. The technique is suitable for use in environments where certain risks, including those risks associated with information security, are present, and has been used in the past to, among others:

- Identify core members and organisations within terrorist groups [18]; and
- Identify hierarchies in criminal Dark Web forums [19].

In addition to the studies mentioned above, SNA has also been used to enhance the information security of an organisation. The work done by Dang-Pham, Pittayachawan and Bruno [20] is of particular interest to this study as it serves to demonstrate the validity of the method discussed here. In the study done by Dang-Pham, Pittayachawan and Bruno, SNA was used to identify individuals who would be able to serve as information security champions. These individuals were then trained in information security so that their influence would help to shape the workplace culture with regards to information security. Because of the importance of this method, it will be referred to as the DPA-method (Dang-Pham Awareness) in the remainder of the paper. SNA has also been used in different studies to identify individuals who pose an organisational risk. By calculating the relative SNA metrics for the various nodes, individuals who may pose a risk due to their position in the network can be identified [21, 22].

The purpose of this paper is to address the information security awareness shortcomings that may exist in university classes and faculties by employing an SNA approach. As the method can be applied to target important individuals and locations using both formal and informal social structures, it should prove useful when developing targeted awareness programmes that can be used to inform staff and students alike. Once these central individuals and locations have been identified, security awareness programmes using classic awareness items such as posters, pens, brochures, discussions, etc. can be used to inform people about security issues and thereby improve security awareness [23]. The purpose of the method proposed in this paper is therefore not to revolutionise traditional security awareness programmes, but merely to provide a way to improve their effectiveness and coverage in situations where security education and –training would not be feasible, and full-scale awareness programmes may be prohibitively expensive, or cause unwanted fatigue.

The remainder of this paper is organised as follows. In the next section, introductory background information with regards to some SNA metrics is provided. This is followed in Sect. 3 with the discussion of the proposed method, and two illustrative examples. A discussion of the findings is presented in Sect. 4, and in Sect. 5 the paper is concluded.

2 Background

2.1 Social Network Analysis

Any social organisation can be considered to be a series of interconnected networks, and as such standard graph modelling can be used to represent them. In such a network, nodes can be used to represent entities, such as people, knowledge, tasks or resources, whereas arcs can be used to represent the relationships that exist between them.

SNA allows for the quantitative analysis of a social organisation through graph theory, and various metrics can be calculated in order to analyse a network. Although a large number of metrics exists (a count of the work done by Clemente, Martins and Mendes [24] shows 28 metrics, whereas the help section of the ORA-Lite software suite names almost 200), only four basic metrics that are used in the illustrative examples will be briefly introduced. The discussion of the four SNA metrics is based on the work done in [21]. Comprehensive discussions of a large number of metrics can be found in a number of sources, such as [24–26].

Degree Centrality. The degree centrality measure is concerned with an individual node and more importantly the particular node's position within the network [21, 27]. A node's ability to influence a particular network is governed by its position within the network, and this in turn is referred to as the node's centrality measure [21]. There are a number of different types of centrality, but the core principle of centrality is that a node that is located more centrally, i.e. has more specific connection types than other nodes, will have a greater specific influence on the network as a whole. One of the quantitative measures used to describe the influence of such a node is referred to as its total degree centrality, and is calculated by using several node properties, such as the number of connections leading into the node, the number of connections leading out of the node,

and the sum of the aforementioned connections [21]. A node with a high total degree centrality would be an excellent target for security awareness training, as any information injected into the network at this point is likely to propagate to the rest of the network in some way.

Closeness Centrality. Closeness centrality is calculated by determining all the geodesic distances (i.e. the shortest distances) to all other nodes within the network [21], and takes all indirect connections to other nodes that a node possesses, together with all direct connections, into account. A node that has a high closeness centrality value is considered to be a good source of information, whereas nodes with a high degree centrality value aids in the diffusion of information throughout the entire network. This means that analysis of the nodes with the greatest closeness centrality values should provide the best information with regard to the information in the network, and would therefore mitigate the need for full node-by-node network analysis.

Betweenness Centrality. When examining interactions between two non-adjacent nodes, the nodes that lie on the paths connecting the two nodes have some control over the interaction between the two nodes [28]. The betweenness centrality measure is a representation of the number of times that a particular node finds itself on the geodesic path of other nodes within the entire network [21]. This measure is reflective of the number of indirect nodes that are connected to a particular node. Thus, a node that has a high betweenness centrality measure would also be a good candidate to use to distribute knowledge and information throughout the network, as these types of node are exclusive, limited sources of information for parts of the network. There is, however, a downside to using such a node: a node with a high betweenness measure is at risk of being overburdened, as such a node would spend a portion, if not all, of its time facilitating interactions between other nodes.

A node that finds itself as an intermediary in an information exchange relationship between two nodes is also considered to be in a position of power, as any information exchanged between the two nodes has to go through the intermediary. The intermediary has a unique position of power in this instance, as it can determine not only the fidelity of the information being exchanged, but also whether information is exchanged at all. Thus, as the number of nodes that relies on such an intermediary increases, so too does the relative power the intermediary node possesses.

Eigenvector Centrality. Eigenvector centrality measures the extent to which a particular node is connected to other nodes that are considered to be highly connected or are of some particular importance [21]. Nodes that have a high eigenvector centrality value are important to note since they are considered to possess emergent leadership properties [29]. Nodes with a high eigenvector centrality are therefore also considered good targets for security awareness, as they tend to take on the roles of early adopters.

2.2 Network Formality

The formality of a network within the context of this paper is a measure of how formal the relationships that are used to construct a social network are. A highly formal network will utilize formal relationships, such as reporting structures, while a less formal network will make use of what is known as informal information systems (IIS). These systems are of particular interest, as they are found in every organisation and present one of the many places where SNA can be applied. IIS are special types of information system that represent the so-called "grapevine" of an organisation [30]. IIS are characterised by their lack of formal structure, their questionable reliability and their possible incompatibility with formal information systems. Unfortunately, due to their ability to collect a significantly greater subset of data, IIS are often crucial to business processes [31, 32]. It is important to take note of these types of information system, as they can have a profound impact on the flow of information within an organisation and must therefore be considered when developing a method that relies on the characteristics of a social network to improve security awareness within an organisation. Depending on the organisation, it may be necessary to target the social networks associated with IIS, rather than those networks associated with its formal structures, in order to obtain the desired results with regards to information security awareness. In an academic environment, for example, it is important to target both the more formal networks that include relationships, such as reporting structures and teaching responsibilities, and the less formal networks, such as those that include social relationships between students.

3 Method

The methodology employed in this paper broadly follows the DPA-method, with a number of notable exceptions:

- The DPA-method uses formal networks constructed from an organisation's hierarchy, whereas the method proposed here targets both formal and informal social networks;
- The method proposed in this study specifically targets personnel and students in an academic setup, such as a university, rather than an organisation; and
- The information security awareness programmes developed using the method in this study can be used to structure a programme that ideally targets the expected awareness level of a group, whereas in the DPA-method a number of influential employees are fully trained in information security awareness.

The proposed method is executed in three primary phases: Preparation, Network Construction, and Evaluation and Implementation. The basic process of the method is shown in Fig. 1.

The first phase, namely the **Preparation** phase, focusses on developing a clear and congruent approach to implementing the method. During this phase, a number of issues crucial to obtaining useful SNA data are addressed. The first of these issues deals with properly "bordering" the group the awareness programme is to target. In an academic environment, bordering may include aspects, such as field of study, the faculty they belong to, their lecturers, etc. This phase also focusses on determining the scope and formality of the networks that will be used.

The **Network Construction** phase is primarily focussed on collecting and processing the network data needed to identify the target individuals. This phase focuses on selecting data collection methods that can be used to construct social networks. These methods may include questionnaires, email-scanning, class-list processing, etc. if a more informal network was selected. Otherwise, formal organisational structures, such as reporting hierarchies can be used, which negate the necessity of using intrusive techniques, such as questionnaires and email-scanning. Once the members of the group have been identified and the nature of the relationships between them has been established, the social network can be constructed. This, along with the calculation of the metrics, is ideally done using software. In this phase, the impact of selecting a more formal or a less formal network will also become clear. Should the impact of the network formality be too great in a negative sense, the Preparation phase should be repeated in order to either negate or mitigate the impact.

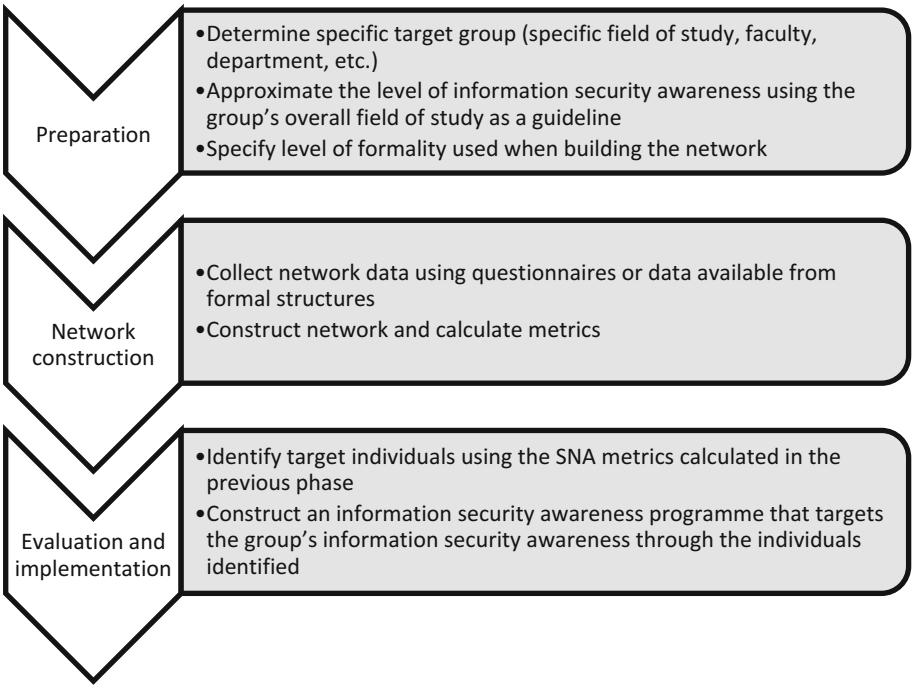

Fig. 1. Process of the proposed method, showing progression through the three phases

During the final **Evaluation and Implementation** phase, the data from the previous two phases are used to determine both the contents of the awareness programme and its intended targets. The specifics of the awareness programme's contents will likely differ from case to case, as the programme should be adapted to the targeted individual, as well as the group in general.

3.1 Illustrative Examples

To illustrate the feasibility of the proposed approach, two practical experiments were conducted. In the first experiment an informal social network construction approach was used, whereas a formal social network was utilised in the second experiment.

Case Study 1. During the Preparation phase a target group of 25 post-graduate students was chosen. An informal social network construction approach was decided upon, as there were no significant formal connections amongst the students apart from attending the same class. In the Network construction phase data were obtained from the students. The following social question was posed to the students:

> *Suppose the computer security group is invited to a function by the industry and everyone shows up. The venue is properly decorated and a number of round tables have been prepared, with exactly one chair for each of the students. If you could make the decision, who would you prefer to have on your right- and left-hand side at the table?*

The response rate was 68%, which was deemed adequate for demonstration purposes.

Respondents were given the option of choosing from a list of names that correspond to the students registered for the class. The data obtained were analysed using ORA-Lite [33], which was also used to construct the network. The four measures discussed in Sect. 2 were calculated and are used in the next phase to determine candidates for disseminating security awareness information through the network. The network obtained is presented in Fig. 2.

During the final Evaluation and Implementation phase, the calculated measures were evaluated to identify candidates that should be targeted. Results indicated that node LR has the highest betweenness centrality at 0.028, eigenvector centrality at 0.322, and total-degree centrality at 0.174, while node CP has the highest closeness centrality at 0.055. These values indicate that the best singular candidate to target would be node LR. An evaluation of the network shown in Fig. 2, however, shows that selecting only node LR will not be entirely effective as there are three distinct, unconnected networks. Therefore, in order to expose the entire network, nodes AG, which is visually the centre of subnetwork B, and node LS in subnetwork C, which has a betweenness centrality of 0.01, an eigenvector centrality of 0.156, and a total-degree centrality of 0.109, should also be targeted.

Case Study 2. For Case Study 2 a formal network construction approach was chosen. The relationships between the personnel at a Computer Science department at a South African university and their formal post-graduate students were used. Where duplicate connections were found, for instance where one student received guidance from more than one member of the department, the weight of the existing connection was increased to indicate a closer relationship. The same three phases used in Case Study 1

were used and the network shown in Fig. 3 was obtained. The data were anonymised, and the node names were chosen to differentiate between students and staff. All node names that contain a D represent staff and all nodes that contain an N represent students. From Fig. 3 as well as the metrics calculated from this network, it is clear that nodes D60, D49, D14 and D76 represent the most connected and influential members in this network. Node D60 in particular has the highest value in all four metrics, which indicates that this person is not only an emergent leader within the network, but is also an influencer. This makes sense as this node is a member of the academic staff who has a large number of students that also receives guidance from other members of staff. Node D76 is also a good target as the node has the second-highest total-degree centrality value. The node does, however, have a significantly lower eigenvector centrality value, and the reduced leadership influence may impact the efficacy of using this node as a target. The ideal situation would involve all four of these individuals, namely D60, D49, D14 and D76, being targeted in information security awareness programmes. As these four individuals are likely to have regular meetings or discussions, any information passed to them should disseminate through the network relatively quickly and naturally.

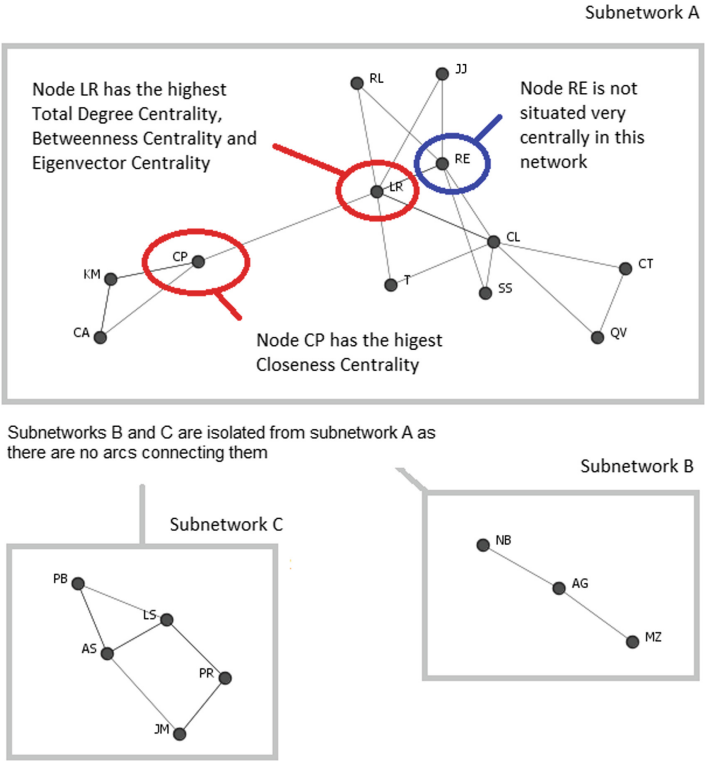

Fig. 2. Social network based on the informal social question

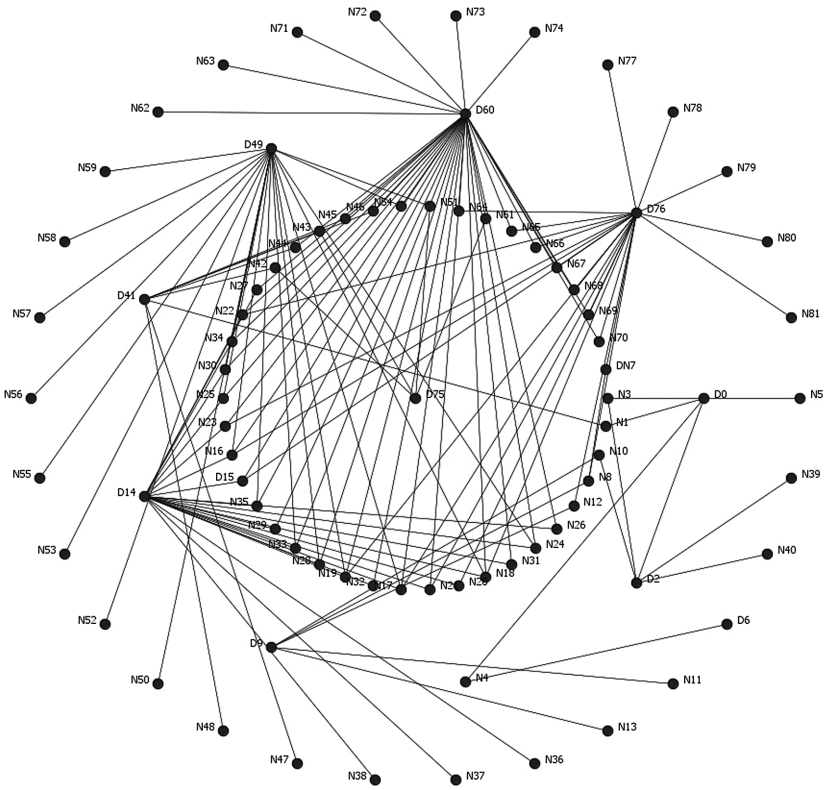

Fig. 3. Formal network of the computer science lecturers and post-graduate students

4 Discussion

The organisational structure of universities generally differs from more traditional organisations in that an academic organisation incorporates a large number of students, which are generally not part of a formal management structure. Universities also differ from other organisational structures in that the various departments at a university are quite often isolated from one another. While it is likely that an administration department may have contact with all the various faculties, it is generally quite rare for separate faculties to have frequent contact with one another. These aspects of an academic organisation make it difficult to target both the staff and the students at a university. While possible in theory, in practice it is difficult to provide information security training to both students and staff, as there is no simple way to organise events of such a size. In addition to the logistical difficulties, neither students nor staff like attending awareness training sessions, especially if there is a perception that no new information will be provided. These problems are further compounded by the financial limitations most universities have to implement in order to remain solvent. Security awareness training for a whole university will likely require significant funds. Such an investment, as far as most universities are concerned, offers too little in return.

The two case studies presented in this paper demonstrate that SNA is a feasible alternative to large scale security awareness programmes in an academic environment, due to a number of reasons. The first of these reasons is that both formal and informal techniques and relationships can be used to construct social networks, which means that there is no absolute dependency on specific structures. This is an advantage in academic environments where a comprehensive formal structure may be limited or non-existent. Another reason is that a handful of individuals can be identified for targeted awareness training. This significantly reduces the cost and, as the topics of the awareness programmes can be selected to correspond to the individual's level of information security knowledge, the chances of fatigue are also drastically reduced. A further advantage is that security awareness can be addressed less formally and more consistently: as new threats are identified, the various targeted individuals can be informed with minimal cost and effort. These individuals will also have a known level of information security knowledge, which will make a continuous programme more effective. SNA is also a relatively simple method to implement, as software packages that implement it do not require overly complex data in order to produce results. This makes the technique relatively easy to implement and use. A final advantage is that any number of networks can be constructed concurrently in order to target a large group. If say, for example, two departments have no contact with one another and their internal organisational structures are too distinct, a network can be constructed for each department using bordering techniques that are appropriate to each department.

5 Conclusion

Information security awareness programmes have to be implemented and used with great care in order to be effective. In more traditional organisations, formal awareness programmes are generally used to address information security awareness shortcomings. In academic organisations, where formal structures do not necessarily include all the members of the organisation, such as students, it is often much more difficult to conduct effective security awareness training. In this paper, in an attempt to address some of the problems of conducting security awareness training in an academic environment, the feasibility of using SNA to develop targeted awareness programmes was investigated. Two illustrative examples, one using formal structures and the other informal relationships, were presented to demonstrate that SNA is a feasible alternative to formal awareness programmes in an academic environment.

The contribution of this study is that the suggested approach, that may be easier and faster to use, and reduce certain limitations, such as costs, fatigue, and the inclusion of information that is inappropriate for the target audience, is indeed feasible. Future work will include the use of more extensive tests, such as the use of larger sample groups and the monitoring of information security levels, to demonstrate the usability of the presented method. These studies will also show how effective, both in terms of cost and coverage, the proposed method is when compared to untargeted, traditional awareness programmes.

References

1. Shillair, R., Cotten, S.R., Tsai, H.S., Alhabash, S., LaRose, R., Rifon, N.J.: Online safety begins with you and me: convincing Internet users to protect themselves. Comput. Hum. Behav. **48**, 199–207 (2015)
2. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput. Secur. **42**, 165–176 (2014)
3. Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: a literature review. Int. J. Inf. Manage. **36**(2), 215–225 (2016)
4. Rezgui, Y., Marks, A.: Information security awareness in higher education: an exploratory study. Comput. Secur. **27**(7–8), 241–253 (2008). https://doi.org/10.1016/j.cose.2008.07.008
5. Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A., Sanchez, D.: From the user's perspective: perceptions of risk relative to benefit associated with using the internet. Comput. Hum. Behav. **59**, 456–468 (2016)
6. Arachchilage, N.A.G., Love, S.: Security awareness of computer users: a phishing threat avoidance perspective. Comput. Hum. Behav. **38**, 304–312 (2014)
7. Aloul, F.A.: The need for effective information security awareness. J. Adv. Inf. Technol. **3**(3), 176–183 (2012)
8. Chen, C.C., Medlin, B.D., Shaw, R.S.: A cross-cultural investigation of situational information security awareness programs. Inf. Manage. Comput. Secur. **16**(4), 360–376 (2008)
9. Thomson, M.E., von Solms, R.: Information security awareness: educating your users effectively. Inf. Manage. Comput. Secur. **6**(4), 167–173 (1998)
10. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Inf. Manage. Comput. Secur. **8**(1), 31–41 (2000)
11. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Comput. Secur. **25**(4), 289–296 (2006)
12. Ng, B., Kankanhalli, A., Xu, Y.: Studying users' computer security behavior: a health belief perspective. Decis. Support Syst. **46**(4), 815–825 (2009)
13. Tsohou, A., Karyda, M., Kokolakis, S.: Analysing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput. Secur. **52**, 128–141 (2015)
14. Boksem, M.A.S., Tops, M.: Mental fatigue: costs and benefits. Brain Res. Rev. **59**(1), 125–139 (2008). https://doi.org/10.1016/j.brainresrev.2008.07.001
15. van der Linden, D., Frese, M., Meijman, T.F.: Mental fatigue and the control of cognitive processes: effects on perseveration and planning. Acta Psychol. **113**(1), 45–65 (2003). https://doi.org/10.1016/S0001-6918(02)00150-6
16. Furnell, S., Thomson, K.-L.: Recognising and addressing 'security fatigue'. Comput. Fraud Secur. **2009**(11), 7–11 (2009). https://doi.org/10.1016/S1361-3723(09)70139-3
17. Scott, J., Carrington, P.J.: The SAGE Handbook of Social Network Analysis, SAGE Publications (2011)
18. Fu, J., Sun, D., Chai, J., Xiao, J., Wang, S.: The "six-element" analysis method for the research on the characteristics of terrorist activities. Ann. Oper. Res. **234**, 17–35 (2015)
19. Philips, E., Nurse, J., Goldsmith, M., Creese, S.: Applying social network analysis to security. In: Working Papers of the Sustainable Society Network, pp. 11–27 (2015)
20. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Applications of social network analysis in behavioural information security research: concepts and empirical analysis. Comput. Secur. **68**, 1–15 (2017)

21. Armstrong, H.L., McCulloh, I.: Organizational risk using network analysis. In: Proceedings of South African Information Security Multi-Conference (2010)
22. Armstrong, H., Armstrong, C., McCulloh, I.: A Course Applying Network Analysis to Organizational Risk in Information Security (2010)
23. Whitman, M.E., Mattord, H.J.: Principles of Information Security. Cengage Learning (2011)
24. Clemente, F.M., Martins, F.M.L., Mendes, R.S.: Social network analysis applied to team sports analysis. SAST. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-25855-3
25. Brin, S., Page, L.: The anatomy of a large-scale hypertextual web search engine. Comput. Netw. ISDN Syst. **30**(1–7), 107–117 (1998)
26. Freeman, L.C., Roeder, D., Mulholland, R.R.: Centrality in social networks: II. Experimental results. Soc. Netw. **2**(2), 119–141 (1979)
27. Hanneman, R.A., Riddle, M.: Introduction to Social Network Methods. University of California (2005)
28. Wasserman, S., Faust, K.: Social Network Analysis: Methods and Applications. Cambridge University Press, Cambridge (1994)
29. Borgatti, S.P.: Centrality and network flow. Soc. Netw. **27**, 55–71 (2005)
30. Clancy, D.K., Collins, F.: Informal accounting information systems: some tentative findings. Account. Organ. Soc. **4**(1–2), 21–30 (1979)
31. MacDonald, S.: Informal information flow and strategy in the international firm. Int. J. Technol. Manage. **11**(1–2), 219–232 (1996)
32. Duncombe, R., Heeks, R.: Enterprise across the digital divide: information systems and rural microenterprise in Botswana. J. Int. Dev. **14**(1), 61–74 (2002)
33. CASOS, "ORA-Lite" (2018). www.casos.cs.cmu.edu/projects/ora