The Lemming Effect in Information Security

D.P. Snyman, H.A. Kruger, and W.D. Kearney

School for Computer Science and Information Systems, North-West University,
Potchefstroom, South Africa
e-mail: {dirk.snyman; hennie.kruger}@nwu.ac.za; kearneys@iinet.net.au

Abstract

This research describes the first investigation of the lemming effect in information security by means of behavioural threshold analysis in practice. The analysis of group dynamic indicates that the lemming effect is indeed present in information security behaviour. The analysis thereof can be employed to assist companies in understanding the manner in which employees influence each other in their behaviour in terms of security. By identifying possible problem areas this approach can also assist in directing their information security education endeavours towards the most relevant topics.

Keywords

Information security; lemming effect; human behaviour; behaviour threshold analysis; group psychology.

1. Introduction

Human aspects of information security studies often aim to investigate the underlying behaviour of the end users that interact with information technology systems (Pham *et al.*, 2017). Quite often such studies look to the manner of interaction with information security, both in terms of individuals' actions and pre-suppositions (McCormac *et al.*, 2017), as well as overarching group dynamics and norms that influence and guide such interactions (Bauer and Bernroider, 2017). Concerning the latter, an interesting phenomenon is that of the so-called "lemming effect". The lemming effect refers to the propensity of individuals to follow the behaviour of a group blindly even when the behaviour is assuredly dangerous (Wiedermann *et al.*, 2014). The term is derived from the behaviour of lemmings (small rodents) that are purported in popular culture to follow migration behaviour of the group blindly, even walking off cliffs in droves only to fall to their deaths. In terms of information security, this would involve individuals following the group example in their information security behaviour.

Even though many previous studies exist that investigate information security behaviour (Crossler *et al.*, 2013; Warkentin *et al.*, 2011) and many behavioural theories (i.e., protection motivation theory, theory of planned behaviour, theory of reasoned action, etc.) have been developed that are often used as basis for these studies (Sommestad *et al.*, 2014), there still seems to be room for further exploration. For instance, Dang-Pham *et al.* (2017) argues that these previous studies mainly focus on individualistic cognition of employees and supply limited contextual details. Furthermore, results and findings are also subject to the theoretical assumptions of the theories employed in the studies (Dang-Pham *et al.*, 2014).

Given the importance of information security and the apparent shortage on approaches that include contextual details, this paper reports a practical application to evaluate the lemming effect by including the context of co-workers instead of focusing on individual cognition on its own. The method that is used to study the lemming effect is based on the application of threshold models of collective behaviour (Granovetter, 1978) and was influenced by the theory of planned behaviour (Snyman and Kruger, 2017a). This method is applied to a large utility corporation in Australia.

The use of behavioural threshold analysis in information security has not been applied in practice before. This paper forms part of a larger research project where the feasibility of behavioural thresholds in information security is investigated. Snyman and Kruger (2016, 2017a) initiated the use of behavioural threshold analysis information security by testing the approach in their exploratory research. They presented the proof of concept as a feasible approach to information security behaviour analysis. This was succeeded by a study on effective data collection methods for threshold analysis (Snyman and Kruger, 2017b). These studies serve as the basis for this research and were used as iterations to refine the process and methodology of behavioural threshold analysis in information security. This current paper differs from the aforementioned initial exploratory research therein that this is the first report on the first practical application of behavioural threshold analysis in information security to be put into practice.

The remainder of the paper serves to describe the process and has the following structure: In Section 2 an introductory background on behavioural threshold analysis is presented. A description of the application of behavioural threshold analysis in information security, with specific reference to the methodology and experimental setup, is shown in Section 3. The results, which were obtained for the experiment described in Section 3, are presented in Section 4 and discussed in Section 5. Finally, Section 6 concludes this report and looks towards future directions for this research.

2. Behavioural threshold analysis

The concept of behavioural thresholds as well as threshold analysis will only be revisited briefly in this section to serve as background information as the concepts were already presented in detail in the previous papers. For a more in-depth review, see Snyman and Kruger (2016).

The foundational idea of behavioural thresholds as presented by Granovetter (1978) is that each individual in a group possesses an internal decision-making mechanism for following group behaviour. This mechanism weighs the personal cost versus gain of participation in the group behaviour, given the number of other group members that are already engaged in the behaviour. The mechanism expresses the willingness to participate as the number of other group members whom should already be participating in the behaviour before the possible gains outweigh the cost for the individual. This is called the individual's behavioural threshold. When it is known to the individual that more group members are participating in the group behaviour than the number represented by their personal threshold, they will also participate in the group behaviour. This corresponds to the lemming effect that was mentioned in the Introduction. Granovetter (1978) explains the working of the mechanism using an analogy as follows: Within a group of workers in an organisation, a rumour might start circulating. An individual might pay little attention to the credibility of the rumour if it is heard from only one source. When more sources impart the same rumour to the individual, the rumour gains credibility because the number of sources is larger than before. The individual's internal mechanism then determines that if the credibility reaches a critical threshold, i.e. enough sources share the rumour; the individual will also believe and circulate the rumour. The individual's threshold has been exceeded and they will take part in the group action. Therefore, the individual has theoretically succumbed to the lemming effect. In the same way it is applicable to information security, e.g. if enough members of a group share their passwords with other members and the number exceeds an individual's threshold for participation, the individual will also share their password with others. To show the working of the model in action and illustrate the advantages thereof, the model was applied in practice and the following section presents the methodology that was followed.

3. Application of behavioural threshold analysis

The behavioural threshold analysis exercise was conducted with 63 respondents from a large utility corporation. From the existing structures at the corporation, three groupings of employees were identified, i.e. permanent staff, contractors, and management. Participation in this study was voluntary and the questionnaire had a specific consent section in line with acceptable practice. All information supplied by the respondents was strictly anonymous. Ethical clearance for the exercise was obtained from the human resources department and the CEO. Each respondent completed an online questionnaire on their willingness to perform certain information security actions, given the number of others whom also perform the actions.

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments used to gather the relevant behaviour data (Snyman and Kruger, 2017b). This is both in terms of the topics of information security questions that are posed to respondents and how these questions are presented typographically. For the purposes of this application, the following six questions were posed to the respondents (see Table 1).

Focus area	Information security behaviour threshold question
1. Security training	How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?
2. Social media use	How inclined would you be to also spend excessive work time on social media, given the percentage of staff that spend excessive work time on social media?
3. Incident reporting	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?
4. Internet use	How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of staff that regularly access dubious websites from devices connected to your company network?
5. Email use	How inclined would you be to also open any unfamiliar email attachments, given the percentage of staff that normally open any unfamiliar email attachments?
6. Password management	How inclined would you be to also share passwords, given the percentage of staff that share their passwords?

Table 1: Information security questions for behavioural threshold analysis

The questions were based on focus areas and topics identified from the Human Aspects in Information Security Questionnaire (HAIS-Q) (Parsons *et al.*, 2017; Parsons *et al.*, 2014). The six focus areas that are shown are neither exclusive nor extensive, but serve to illustrate the suitability of a focus area and related question for behavioural threshold analysis. Depending on the intention of the specific behavioural threshold analysis exercise that is to be conducted, different suitable focus areas (for instance mobile computing) may be identified. For instance, the first focus area and related question in Table 1 is in contrast to the others as it describes positive behaviour, i.e. volunteering for information security training. This focus area and question was added as a control to test the willingness of the respondents to follow others in their behaviour if there was no negative connotation to performing the behaviour. Furthermore, the focus areas of the HAIS-Q are divided into questions that address different aspects of the themes. The *Password management* focus area has questions on “password sharing”, “re-using passwords” and “strong passwords” (Parsons *et al.*, 2017). Depending on whether a study has an interest in these specific aspects, they may also be included. However, special attention should be given to the number of questions that are included as each question necessitates ten new responses. Owing to the number of responses, adding an extra question places a relatively higher burden on the respondent in comparison with traditional questionnaires. The number of questions is also contrasted to traditional approaches where multiple questions are employed to test a given aspect (Sekaran and Bougie, 2010). The nature of this model only allows for one question per aspect: *Will you participate if enough others do?*

Each of the questions from Table 1 was answered on a scale of inclination for participation in the specific information security activity, given the percentage of other group members that are known to partake in the activity. An example is presented in Table 2.

Percentage of staff that ignore security incidents by not reporting them.	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?			
	Never	Somewhat inclined	Strongly inclined	Always
0—10%	1	2	3	4
11—20%	1	2	3	4
21—30%	1	2	3	4
31—40%	1	2	3	4
41—50%	1	2	3	4
51—60%	1	2	3	4
61—70%	1	2	3	4
71—80%	1	2	3	4
81—90%	1	2	3	4
91—100%	1	2	3	4

Table 2: Example of a complete behavioural threshold question

It should be noted that the sample size in this exercise does not follow traditional style for questionnaires which can be summarised as “the more the better”. Due to the unique nature of behavioural threshold analysis, it is specifically done in smaller groups. The members of the group have to be aware of the habits and behaviour of others in order to answer the questions about their own thresholds (Growney, 1983). When sample sizes become too large (i.e. start to extend beyond the natural boundaries of organisational departments) the group members no longer have the awareness that is crucial for the correct application of the model and the probability of incorrect answers increases.

As mentioned earlier in Section 2, the threshold for an individual is the number (percentage) of others that have to exhibit a specific behaviour before they will join in. If a respondent indicated that they would be somewhat inclined to participate, given the percentage of the group that do so, that percentage was taken as their individual threshold. This was noted for each respondent and the aggregate of all the respondents’ thresholds was used for the behavioural threshold analysis results (see Section 4).

In the earlier, related studies, it was noted that the results might have been affected by social desirability and was ascribed to the sensitive nature of the information security questions being asked as well as how familiar the respondents were with the topics (Snyman and Kruger, 2017a, 2017b, 2016). Social desirability refers to the tendency that many respondents have to answer questions in a manner that they think to be acceptable, rather than truthful (Fisher, 1993). It was therefore deemed necessary to control for this phenomenon to obtain a more accurate view on the predicted group behaviour. A series of additional questions were given to the respondents after completion of the behavioural threshold questionnaire to determine the level of social desirability that they exhibit. The questions to measure social desirability were based on a standardised 33-question measurement instrument, which was developed by Crowne and Marlowe (1964) and later shortened to eight questions by (Ray, 1984). These eight questions were used to measure social desirability in this research. They are presented in Table 3 below.

Social desirability questions
1. Are you always courteous, even to people who are disagreeable?
2. Are you always a good listener, no matter whom you are talking to?
3. Are you quick to admit making a mistake?
4. Have there been occasions when you took advantage of someone?
5. Do you sometimes try to get even rather than forgive and forget?
6. Do you sometimes feel resentful when you do not get your own way?
7. Are you always willing to admit when you make a mistake?
8. Have you sometimes taken unfair advantage of another person?

Table 3: Social desirability questions (Ray, 1984)

The social desirability questions are simply answered with Yes, No, or Unsure. Depending on the specific question either Yes or No will be awarded a score of one or three respectively. Unsure is always scored two. The scores for all of the questions is added together for a score out of a possible 24. The higher the score, the higher the likelihood is that the respondent's answers were influenced by social desirability. For the purposes of this study, only the extreme score of 24 is taken to mean that the respondent was not truthful in the way in which they answered the questions. If a respondent was deemed untruthful, their answers on the information security questions were adjusted towards a higher level of inclination for participation (see Table 2). The level of willingness for participation was adjusted one level higher, i.e. if a respondent with a social desirability of 24 selected their inclination of participation as *somewhat inclined (2)* it was adjusted to *strongly inclined (3)*. This would mean that the individual's threshold for participation is taken at a lower percentage in the cases where the behaviour is seen as a negative information security action. The reverse holds true for positive information security behaviours where the respondents might overstate their willingness for participation. In these cases, the threshold for participation is taken at a higher percentage. For all of the questions in this study, both the adapted and the original thresholds are taken into account in order to illustrate the effect of the adaptation.

The information security behavioural threshold analysis exercise was executed as explained above and following an analysis of the collected data, the results are presented in the following section.

4. Results

This section shows the aggregation of the information security behavioural threshold analysis results that were obtained from the respondents. Due to page restrictions, the results for all of the questions cannot be graphically presented and it was decided that only half of the results (i.e. three questions) will be presented in the behavioural threshold graph format, however, Section 5 presents a discussion of the results that were obtained for each remaining three questions.

The aforementioned graph format represents a plot of the cumulative behavioural thresholds for a corresponding question plotted against a uniform distribution of thresholds called the equilibrium line. The shape of the behavioural threshold graph and the intersection with the equilibrium line allows for an interpretation that may predict a percentage of members of the group that may eventually participate in the relevant information security behaviour. It should be noted that a detail analysis of all the nuances conveyed by the graph is omitted due to page restrictions and only the crux of the analysis is presented. An overview of other measures and analyses (e.g. information conveyed by gradient measurement of the graph) is presented in (Snyman and Kruger, 2017a).

The results for the three questions that are presented in detail (namely questions 1, 3, and 6 from Table 1), were chosen due to their illustration of 1) the willingness of individuals to follow the positive information security behaviour of others; 2) a situation where the group appears to be unaware of the topic's security issues and individuals are easily influenced to follow the negative information security behaviour of others, in other words where individuals exhibit low thresholds for participation; and finally 3) a situation where the group seems to be sufficiently security aware and individuals should not be easily convinced to follow the bad information security behaviour of others, in other words where individuals exhibit high thresholds for participation. The results are presented one by one in this order.

1) Figure 1 shows the cumulative results for the groups' individual thresholds towards question 1 from Table 1 (hereafter referred to as Q1): *How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?*

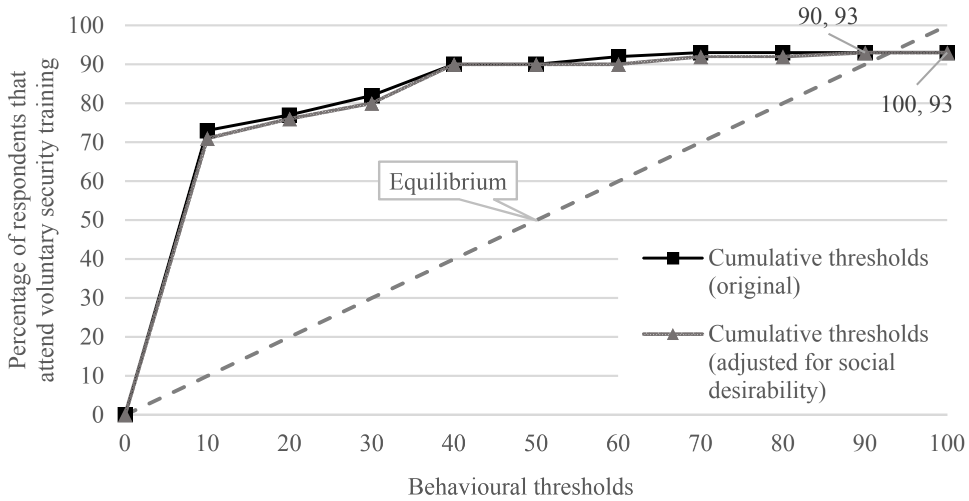

Figure 1: Distribution of behavioural thresholds for Q1

Q1 is an example of a positive influence that members of the group have on one another in the context of information security training. The steep incline and rapid growth in the cumulative behavioural thresholds indicates a *high* willingness (i.e. *low* thresholds) in the members of the group to follow the example of others to also participate in voluntary information security programs. The intersection with the equilibrium line indicates that if the status quo is sustained that the percentage of members that voluntarily participate in security training programs is likely to grow until 93% of the group takes part. The situation is then unlikely to change as the distribution of thresholds reaches satiety at this point.

2) Figure 2 is a representation of the cumulative thresholds reported for question 3 (Q3) from Table 1: *How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?* Q3 is an example where the influence of the group would be considered negative. Participation in the behaviour is not recommended as a good practice to promote high levels of information security. In contrast to the steep incline noted in Figure 1, the slower growth in the distribution of cumulative thresholds indicates that the members of the group are less willing than for Q1, but willing none the less, to follow example of others and participate in the group behaviour of not reporting security incidents.

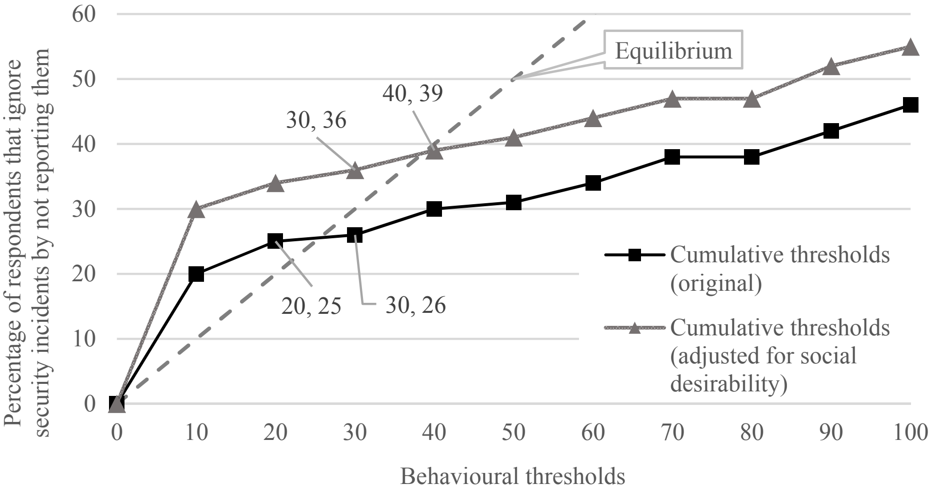

Figure 2: Distribution of behavioural thresholds for Q3

The intersection of the equilibrium line indicates that participation is likely to grow due to the *low* individual thresholds in the group. Participation stabilises with only 39% of the members of the group participating. This distribution of thresholds satisfies the requirements for equilibrium (Snyman and Kruger, 2017a) and the participation rate is unlikely to change unless there is some external influence, like an intervention, that changes the group dynamic.

3) To illustrate the aggregated thresholds for question 6 from Table 1 (Q6: *How inclined would you be to also share passwords, given the percentage of staff that share their passwords?*), Figure 3 is presented. Q6 denotes another example of a negative influence of group behaviour on the individual.

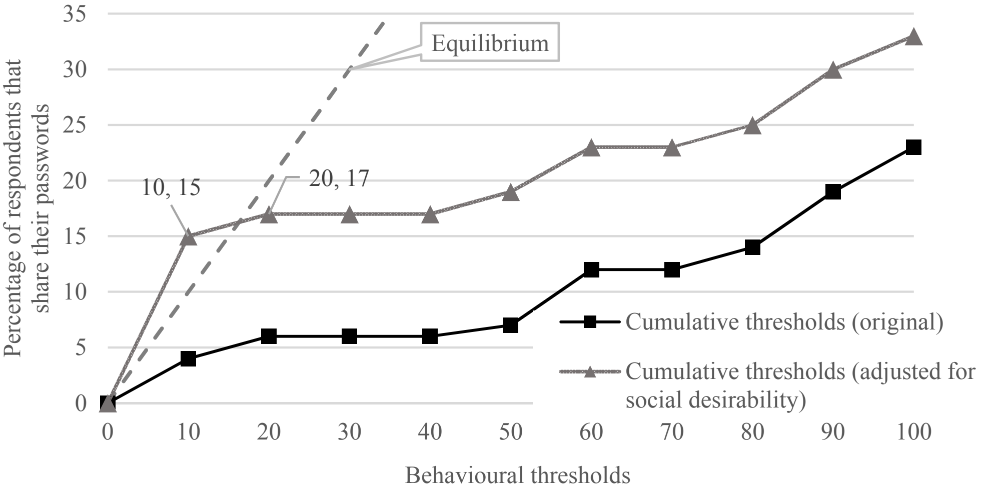

Figure 3: Distribution of behavioural thresholds for Q6

The results for Q6 indicate that the respondents are not willing to follow others in sharing their passwords. The group's unwillingness for participation is because the individual thresholds noted for this example are *high*. The distribution of the original behavioural thresholds never reaches an equilibrium and is indicative of a "dying" behaviour, i.e. no one in the group is likely to exhibit this behaviour. This is indicative of high levels of awareness about the topic conveyed by successful communication through security awareness programs. When the effects of social desirability are taken into account and the thresholds are adjusted, the threshold line intersects the equilibrium line with 17% of the group possibly sharing their passwords.

5. Discussion

Based on the results that are reported in Section 4, this section provides a twofold overview. A discussion is presented in terms of issues relating to this specific research exercise and then remarks of a more general nature relating to behavioural threshold analysis and the lemming effect.

5.1. Specific remarks

The group that was surveyed in this study is shown to be well versed in good information security behaviour. They furthermore exhibit a willingness to be team players in positive behaviour that promotes information security. In spite of the predominantly positive results, there are still some security topics where the lemming effect is observed. One example is the behaviour that was reported for Q3 (Figure 2) in the previous section. The lemming effect causes the individuals to follow group behaviour in not reporting security incidents.

Three questions were already discussed in Section 4, namely Q1 (*security training*), Q3 (*incident reporting*), and Q6 (*password management*). Once again, for space considerations they are omitted in this instance. In the remaining questions that were posed to the respondents, they exhibited high levels of security awareness in terms of the information security aspects that the questions were based on. The analysis show generally positive results for two of the remaining three questions from Table 1, i.e. *internet use* (Q4), and *email use* (Q5) where the respondents showed *high* threshold levels. They will therefore not easily follow harmful group behaviour in these specific instances. This also points to high levels of security awareness (and good information security training) of staff for these two topics. However, for *social media use* (Q2), the recorded thresholds for participating in-group behaviour were noted to be *low* and individuals are therefore likely to follow the group in its bad behaviour. The topics of *social media use* and *security incidents* should therefore be reviewed by the corporation and reaffirmed through security awareness campaigns.

It was also interesting to note that the respondents exhibit high levels of social desirability. The average social desirability score for the participants was measured at 19/24. Such a high score indicates that there is a high probability that the respondents did not answer the questionnaire in a completely truthful manner. High social desirability might indicate that the respondents overstated their good information security behaviour and understated the negative behaviour that they would rather present in a better light. This can be attributed to the sensitive nature of the information security topics included in the questionnaire. The individual might also already be aware of expected behaviour and answers in accordance thereto.

Information security awareness programs serve to educate the members of an organisation of the potential information security threats. They also serve to promote good practices and identify practices that should be avoided. In the case of *social media use* and *incident reporting* it was observed that a percentage, 31% and 39% respectively, of the group is likely to be inclined to participate in negative information security practices. By including topics relevant to this behaviour in information security awareness programs, the percentage should see a decrease. It was shown that the group is willing to participate in such programs, even doing it voluntarily. This should contribute to the success of security awareness programs that are conducted in the corporation.

5.2. General remarks

The results show that the individual in a group is likely to follow the majority example in specific cases with reference to group information security behaviour. This indicated that the lemming effect is indeed present and, when analysed, can be useful to help evaluate group information security behaviour. Behavioural threshold analysis provides a formal measure to capture contextual information for an individual's security behaviour concerning the behaviour of co-workers. This context provides a broader view on information security behaviour than the traditional focus on individual cognisance. By measuring the lemming effect and predicting probable group behaviour, it provides a tool to identify possible risk areas. The identified risks can help focus the efforts of information security awareness programs.

Given the positive contributions of behavioural threshold analysis there are some points that still warrant careful consideration. Collecting data for behavioural threshold analysis poses a unique challenge to elicit useful answers from respondents. As mentioned earlier, the sensitive nature of information security questions often leads to high levels of social desirability. By tailoring the data collection instrument for this specific application the occurrence of social desirability can be somewhat addressed. Furthermore, the uniqueness of the instrument does not allow it to be tested for statistical validity and reliability as with traditional questionnaires. This is due to the specific manner in which the questions are structured to determine the respondent's behavioural threshold. The answers that the respondents provide may also vary to a large degree where they are often completely willing to follow the behaviour of others, or completely opposed to it. Another factor to keep in mind is the relative levels of influence that different members of the group have. An individual might be more inclined to follow the example of friends or prominent figures as opposed to just another employee they barely know.

6. Conclusion and future work

This paper presented the first application of information security behavioural threshold analysis to measure the lemming effect in practice. Given the number of factors that have an influence on this analysis the results should be handled carefully. Further research into these topics is warranted. Consideration might be given to other social theories that explain the influence of a group on an individual such as social capital theory and social cognition theory. The aforementioned notwithstanding, the results indicate the presence of the lemming effect in information security behaviour and that the effect can be measured with the use of behavioural threshold analysis as presented in this research. Furthermore, the results give a good indication of the levels of security awareness of the group in question and helps determine areas in which awareness still needs development.

7. References

Bauer, S. and Bernroider, E.W. (2017), "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization", *Data Base for Advances in Information Systems,* Vol. 48, No. 3, pp. 1-24.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future Directions for Behavioral Information Security Research", *Computers & Security,* Vol. 32, No. 2013, pp. 90-101.

Crowne, D.P. and Marlowe, D. (1964), "The Approval Motive"*, Wiley*, *New York.*

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2014), "Towards a Complete Understanding of Information Security Misbehaviours: A Proposal for Future Research with Social Network Approach", *Australasian Conference on Information Systems (ACIS).*

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017), "Applications of Social Network Analysis in Behavioural Information Security Research: Concepts and Empirical Analysis", *Computers & Security,* Vol. 68, No. 2017, pp. 1-15.

Fisher, R.J. (1993), "Social Desirability Bias and the Validity of Indirect Questioning", *Journal of Consumer Research,* Vol. 20, No. 2, pp. 303-315.

Granovetter, M. (1978), "Threshold Models of Collective Behavior", *American Journal of Sociology,* Vol. 83, No. 6, pp. 1420-1443.

Growney, J.S. (1983), "I Will If You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior", *Modules in Undergraduate Mathematics and Its Applications - Tools for Teaching,* Vol. No., pp. 108-137.

Mccormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual Differences and Information Security Awareness", *Computers in Human Behavior,* Vol. 69, No. 2017, pp. 151-156.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., Mccormac, A. and Zwaans, T. (2017), "The Human Aspects of Information Security Questionnaire (Hais-Q): Two Further Validation Studies", *Computers & Security,* Vol. 66, No. 2017, pp. 40-51.

Parsons, K., Mccormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (Hais-Q)", *Computers & Security,* Vol. 42, No. 2014, pp. 165-176.

Pham, H., Brennan, L. and Richardson, J. (2017), "Review of Behavioural Theories in Security Compliance and Research Challenge", *Proceedings of the Informing Science and Information Technology Education Conference, Vietnam*, COHEN, E., ed., Santa Rosa, CA, USA, Informing Science Institute, pp. 65-76.

Ray, J.J. (1984), "The Reliability of Short Social Desirability Scales", *The Journal of Social Psychology,* Vol. 123, No. 1, pp. 133-134.

Sekaran, U. and Bougie, R. (2010), "Research Methods for Business: A Skill Building Approach"*, John Wiley & Sons*.

Snyman, D.P. and Kruger, H.A. (2016), "Behavioural Thresholds in the Context of Information Security", *Tenth International Symposium on Human Aspects of Information Security & Assurance*, CLARKE, N. L. & FURNELL, S. M., eds., Frankfurt, Germany, Plymouth University, pp. 22-32.

Snyman, D.P. and Kruger, H.A. (2017a), "The Application of Behavioural Thresholds to Analyse Collective Behaviour in Information Security", *Information & Computer Security,* Vol. 25, No. 2, pp. 152-164.

Snyman, D.P. and Kruger, H.A. (2017b), "Optical Polling for Behavioural Threshold Analysis in Information Security", *International Conference on Information and Knowledge Engineering (IKE'17)*, ARABNIA, H. R., DELIGIANNIDIS, L., HASHEMI, R. & TINETTI, F. G., eds., Las Vegas, USA, CSREA Press, pp. 39-45.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies", *Information Management & Computer Security,* Vol. 22, No. 1, pp. 42-75.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention", *European Journal of Information Systems,* Vol. 20, No. 3, pp. 267-284.

Wiedermann, W., Niggli, J. and Frick, U. (2014), “The Lemming-Effect: Harm Perception of Psychotropic Substances among Music Festival Visitors”, *Health, Risk & Society,* Vol. 16, No. 4, pp. 323-338.