# Theorising on Information Cascades and Sequential Decision-making for Analysing Security Behaviour

D. P. Snyman and H. A. Kruger
*School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom, South Africa*

Keywords: Information Cascades, Sequential Decision-making, Information Security, Human Behaviour.

Abstract: Human behaviour is an ever-present aspect in information security and requires special attention when seeking to secure information systems. Information security behaviour is often based on an informed decision where information is obtained by previous experience and observation of the behaviour of others. In this research, the concept of sequential decision-making is contextualised in terms of information security behaviour. Information cascades, which are based on sequential decision-making, are theorised as a model to explain how decision-making (i.e. behaviour) takes place in terms of information security. A case study is presented to illustrate how behavioural threshold analysis can be employed as an instrument to evaluate the effect of information cascades and sequential decision-making on information security behaviour. The paper concludes by theorising on the applicability of the models and approaches that are presented in this research.

## 1 INTRODUCTION

A long-standing approach for protecting information systems was a focus on technical solutions. It was soon realised, however, that technical solutions alone were not sufficient to protect the systems and information from those who intend to access it without due authorisation (Arce, 2003; Lineberry, 2007; Soomro et al., 2016). Humans are inextricably linked to the creation and use of information systems. They are fallible by nature, and it is precisely this innate fallibility that can cause vulnerabilities in information systems, even when the systems are sufficiently protected by technological means (Glaspie and Karwowski, 2017). In a recent publication on information security threats, human conduct (mostly inadvertent behaviour) was responsible for more than two thirds of reported breaches in 2017 (IBM Security, 2018). These behaviours ranged from human error in server configurations, to human compliance with phishing attacks.

In order to attempt to address the human factor in information security, the phenomenon of human behaviour should first and fore mostly be understood. Researchers have long been seeking ways to formalise the study of human behaviour which gave rise to many theories and models that try to explain how behaviour is determined (Granovetter, 1978; Ajzen, 1991; Wilson, 1999; Kroenung and Eckhardt, 2015; Pham et al., 2017; Ooi et al., 2018). Such models are then used in an attempt to explain behaviour in terms of information security. Examples of the most prevalent of such models that have been used in this context include: The theory of reasoned action, the theory of planned behaviour, protection motivation theory, and general deterrence theory (Lebek et al., 2013; Pham et al., 2017).

These models aim to incorporate influencing factors that are intrinsic to an individual and describe how these factors contribute to the eventual behaviour. Ultimately, the behaviour that is performed is based on an informed decision by the individual. The application of the abovementioned models places a person in isolation, but this is seldomly, if ever, the case in a real-world situation.

The theories fail to consider the influence that the decisions of others might have on an individual. When decisions are no longer made in isolation, the direct application of these theories becomes problematic because the motivations for exhibiting a certain behaviour is no longer only an intrinsic one, but extrinsic factors now come into play. Information on the everyday decisions of others are



Snyman, D. and Kruger, H.
Theorising on Information Cascades and Sequential Decision-making for Analysing Security Behaviour.
DOI: 10.5220/0007258702050212
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 205-212
ISBN: 978-989-758-359-9

typically overt for an individual to observe, for instance, the choice in clothing brand, restaurant preferences, etc. These decisions in turn help determine the way in which someone would make his/her own decisions.

Information security behaviour is similarly based on an informed decision as mentioned above. Behaviour in this context is also not confined to an individual's intrinsic motivations but is similarly informed by the decisions that others make. The process of decision-making is often of a sequential nature, i.e. one decision informs the next, which in turn informs another. An individual bases future decisions on the knowledge of previous decisions.

Easley and Kleinberg (2010) describe the use of information cascades to formally model iterative, sequential decision-making of an individual in relation to decisions in a group. Information cascades, in short, refer to how an individual makes decisions (sequentially) based on the probability that the decision is correct, given the decisions previously made by others. This approach has never been used before to model information security behaviour but has been mentioned as a possible problematic phenomenon in relation to privacy and security (see Chesney and Citron (2018) on so-called "deep fakes" for a recent mention of information cascades in literature). Therefore, this paper aims to theorise on the applicability of information cascades as a technique to analyse information security behaviour.

The remainder of this paper is structured as follows: In **Section 2** an overview of the concept of sequential decision-making is presented, followed by an illustrative case study in **Section 3**. **Section 4** consists of a reflection on the implications of the study as well as the key contributions of this research is highlighted. The paper is concluded in **Section 5**.

# 2 SEQUENTIAL DECISION-MAKING

In this section, the concept of sequential decision-making is presented in a twofold manner. Firstly, sequential decision-making is discussed in terms of the information cascades model. Secondly, behavioural threshold analysis is presented as a possible instrument to measure sequential decision-making in information cascades, specifically in terms of information security.

## 2.1 Information Cascades

As mentioned in Section 1, information cascades refer to a formal expression of the process of sequential decision-making. The first mention and the development of information cascades (also called herd behaviour (Banerjee, 1992)) has its origins in the field of Economics to describe, among other things, investment decisions and consumer fads (Bikhchandani et al., 1992; Welch, 1992).

For the sake of the arguments of this paper, a simple, general, description of information cascades is subsequently presented. The aim of this description is to provide a high-level overview of the model and to create an analogy to relate information cascades to information security. The description is based on the explanation of Easley and Kleinberg (2010). They provide a more detailed explanation with mathematical substantiation of the model for further reading.

The decisions of a person are informed by signals, i.e. information, in relation to an expected gain. These signals come in two forms, namely private- and public signals. A private signal is information that is currently known to the person, be it a belief or a fact. When a person makes a decision in isolation, a private signal is what determines the outcome of the decision. When the signal aligns with an associated gain and is powerful enough to overcome the risk associated with potential loss, the decision is made solely on the information conveyed by the signal.

Easley and Kleinberg (2010) note that everyday decisions are rarely made in isolation from the rest of society. Information can be conveyed by signals that are formed extrinsically. Such public signals are based on information that does not come from the individual, but rather from the observation of the decisions that others have made. In a public setting, both private- and public signals will inform the decision. If the signals indicate the same course for the decision, the outcome is obvious but if the two signals provide contrasting information, the strongest signal will inform the decision. It is important to note that both signals are normally imperfect and do not convey infallible information. The signal is always weighed against the probability that the corresponding course for the decision will result in gain, rather than loss.

Due to the sequential nature of decision-making, the public signal becomes stronger with each decision that was made in its favour. The decision-maker is aware of all the public decisions, each one informed by the previous. As a result, the perceived

probability that the public signal suggests the "correct" course for the decision becomes higher.

The main premise of the model, therefore, is that the public signal will almost always prove stronger and influence the decision even when the private signal initially informed a contrasting course.

Information cascades rely on four prerequisites for the model to be applied to a situation (Easley and Kleinberg, 2010):

1) There is a (binary/contrasting) decision to be made;
2) Each person has a private signal that originally informs their initial proclivity;
3) The decisions that were made by others can be observed and the decisions happen sequentially; and
4) The private information of others is not known to the individual.

However, inferences can be made about another's private information based on their publicly noticeable decision from number 3 above.

Take, for instance, an example of adopting new technology. An individual, let us call him John, is looking for a new digital device and has an expectation of the utility (gain) that the new technology will have to him. He reads an online review of the device which indicates that the technology is in its infancy and it might be better to wait for revisions, rather than adopt the technology in its current form. John then forms a negative, personal signal because of the perceived lack of utility. The information that the signal relays prevents him from adopting the technology.

As stated before, John is not in isolation. He moves around in public spaces and notices that another person has one of the devices in their possession. He has, however, no sense of whether the other person is happy with the purchase (i.e. the decision to adopt was the correct decision to make), and he does not know what the private signal of the other person was that convinced him/her to adopt the technology. Instead, John receives a positive public signal that indicates that adoption of the technology has happened. As he encounters and sees more people that have adopted the technology, the higher the probability becomes that adoption, rather than rejection, is preferable and the signal becomes stronger.

As soon as the public signal becomes stronger than the private and overcomes the associated risk with adoption, John will make the decision to follow the group of adopters and adopt the technology. The prerequisites for an information cascade, mentioned above, have been met and an information cascade has taken place.

An example of how information cascades can be evaluated and, possibly, predicted is the application of behavioural threshold analysis. This is discussed in the following sub-section.

## 2.2 Behavioural Threshold Analysis

From the brief description in Section 2.1, it is clear that information cascades and sequential decision-making may play a significant role in information security behaviour. However, to do a meaningful evaluation thereof, in a way that provides new insights into information security behaviour and specifically paradoxical information security behaviour, an acceptable method for analysing information cascades should be found. One possible approach is to use behavioural threshold analysis which is also based on sequential decision-making. In this section, behavioural threshold analysis is introduced briefly as a possible instrument to evaluate information cascades. Parallels are also drawn between information cascades and behavioural threshold analysis to support the idea of behavioural threshold analysis as an evaluation instrument for information cascades and, specifically, sequential decision-making.

The notion of behavioural threshold analysis predates the conceptualisation of information cascades by some time. Behavioural threshold analysis was first developed by Granovetter (1978) and was coined "threshold models of collective behaviour". The premise supporting the model of threshold analysis, is that the behaviour of an individual (Sarah) in a group setting will be influenced by the group's behaviour if a large enough number of other members of the group exhibit a specific behaviour. The number of others that must perform a behaviour before Sarah joins in, is determined by her inherent threshold for participation. If the number of others in the group that perform a certain action, exceeds Sarah's threshold for participation, she will follow the group and also perform the action. To demonstrate the similarities between information cascades and behavioural threshold analysis, an example of behavioural threshold analysis (in terms of information security behaviour) is presented.

Information cascades, in information security behaviour, can manifest itself when employees in a group setting, follow the security behaviour of others rather than relying on their own knowledge. This is similar for behavioural thresholds:

Information security awareness training is often conducted in organisations to educate employees on

basic security hygiene (Alshaikh et al., 2018). Topics such as password sharing, incident reporting, and responsible social media use are commonly addressed in these training programs. Sarah has undergone the training, and she internalises the content. She forms an informed opinion on the related practices and the associated risks (comparable to the risk/gain from information cascades that was mentioned earlier). When she is confronted with either performing, or abstaining from a certain information security behaviour, a contrasting decision (as with information cascades) is to be made. Sarah is not in isolation and she is aware of the actions that other people in her group perform (public signal). Her inherent threshold for participating in the behaviour (private signal) will be weighed against the number of others in the group that perform the action. Sarah *is not* aware what the motivations of the other group members (i.e. their own private signals) are for why they exhibit the behaviour, but she *is* aware of what their decision for behaviour was. If her threshold number (private signal) is exceeded by the number of group members (public signal), Sarah will follow the group example for the behaviour.

This parallel between the two models indicate that they are both applicable to sequential decision-making. The situations in which behavioural threshold analysis can be performed, satisfy the prerequisites for an information cascade to occur, i.e. both models depend on a person to make a contrasting decision, given both intrinsic and extrinsic evidence that inform the decision. Finally, the intrinsic basis for said evidence is not known, but the evidence is clear to see.

Behavioural threshold analysis therefore seems like a feasible approach to provide a mechanism by which information cascades may be evaluated. In the following section, a case study is presented to support this claim.

# 3 ILLUSTRATIVE CASE STUDY

To illustrate how behavioural threshold analysis can be used to evaluate information cascades, a case study was conducted and is presented below in terms of the experimental setup, followed by the results obtained.

## 3.1 Experimental Setup

Behavioural threshold analysis depends on the availability of information about the thresholds of the the members of a group (Granovetter, 1978). One way to obtain their threshold information is by surveying the group by means of a self-reporting questionnaire (Growney, 1983). An exploratory study (Snyman and Kruger, 2016) on the application of behavioural threshold analysis in the context of information security has, however, determined that the measurement instrument that was offered by Growney may not be suitable when applied in a context which is sufficiently different from its initial intended use. This has prompted on-going reflection on, and development of, a measurement instrument for use in this specific context. In its current form, the instrument suggested by Growney (1983) asks respondents to directly nominate their threshold for the number of group members that have to perform an action before they will follow suit. Snyman and Kruger (2016) found that respondents were confused by this style of questioning which lead to inaccurate responses. For this research, based on the ongoing development, it was opted to alter the measurement instrument in order to guide the respondents in answering what their thresholds are. This was achieved in the following way:

The respondents were asked to rate their willingness to follow the group example on a four-point Likert scale, i.e. *1. Never*, *2. Somewhat inclined*, *3. Strongly inclined*, and *4. Always*. Their willingness for participation in the group behaviour was recorded for different threshold level intervals, e.g. rate your willingness to not report security incidents if 31-40% of group members fail to report security incidents. Formally, the question was presented as follows:

*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?*

An example of how the question, response scales, and threshold intervals are incorporated in an online questionnaire is presented in Figure 1.

In order to determine the minimum threshold level for participation, all responses of a *2. Somewhat inclined* and above for a specific threshold interval were taken to mean that the respondent will be influenced by the group if that percentage of group members participate in the specific action. For this illustrative case study The abovementioned approach was applied in a real-world setting by distributing an online questionnaire to contract employees within a company. The identity and other information of the company is not revealed to comply with a confidentiality agreement.

The employees whom were surveyed, typically

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?** *

| | 1. Never | 2. Somewhat inclined | 3. Strongly inclined | 4. Always |
|---|---|---|---|---|
| 0-10% | | | | |
| 11-20% | | | | |
| 21-30% | | | | |
| 31-40% | | | | |
| 41-50% | | | | |
| 51-60% | | | | |
| 61-70% | | | | |
| 71-80% | | | | |
| 81-90% | | | | |
| 91-100% | | | | |

Figure 1: Example of questionnaire layout.

work together in a group (in a departmental setting). They were asked to rate their willingness to participate in group information security behaviour that relates to the non-reporting of information security incidents. Willingness, in this context, relates to the likelihood that an individual will not report a security incident, given the number of other group members that also do not report security incidents.

Responses were obtained from a group of 33 employees. Contrary to the typical expectation for sample sizes relating to questionnaires, the nature of behavioural threshold analysis actually *requires* a smaller number of respondents but all the while imposes another unique requirement: The group members are required to have a knowledge of the behaviour of the other group members (recall the discussion on public signals from Section 2). This requirement determines that behavioural threshold analysis be performed with a group that have regular interaction with one another. In a company setting, this typically relates to business units or departments. Furthermore, the analysis of responses and any group behaviour prediction that is based thereon, is only applicable to the group that was surveyed and therefore the findings of behavioural threshold analysis are not generalised to a greater population. This means that regular guidelines of sample size versus greater population size do not apply in this context.

The behavioural thresholds were noted for each respondent after which a graph of the cumulative distribution of thresholds was constructed (see Figure 2). In the next section, the results that were obtained for the experiment are presented and discussed in short.

## 3.2 Results

Figure 2 shows the employees' cumulative behavioural thresholds for not reporting security incidents, given the number of others that do not report security incidents. On the y-axis, the percentage of participants in the behaviour is shown. The x-axis represents the different threshold-levels, also expressed as a percentage, e.g. the point X on the graph indicates that 36% percent of the group will not report security incidents if 30% of the group do not report such incidents. The different cumulative threshold levels that are shown, were joined with a line to aid in the interpretation of the graph. A uniform cumulative distribution of thresholds was also plotted on the graph as a dotted line. This in known as the equilibrium line. The equilibrium line refers to a collection of points with equal numerical coordinates (Granovetter, 1978; Growney, 1983), i.e. $x=y$ where the number of participants in a behaviour and the threshold levels intersect. When the number of participants becomes equal to an individual's threshold level, they will start to participate in the group behaviour.

When the threshold line (i.e. the cumulative distribution function $F(x)$) intersects with the equilib-

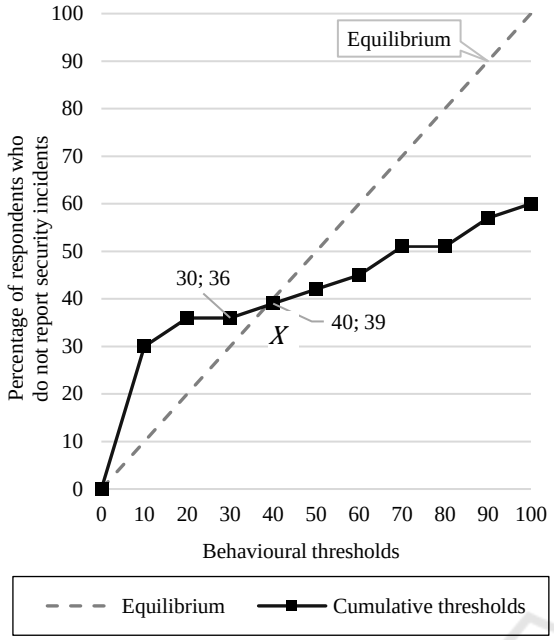


Figure 2: Cumulative threshold graph for information security behaviour (incident reporting).

rium line, where $F(x)=x$, certain inferences can be made about the group behaviour, based on the line-segments to the left and right of the intersection (Granovetter, 1978; Growney, 1983). The gradient of the line-sections determines whether a stable equilibrium is reached. When a stable equilibrium is reached, the number of participants (y-axis) at that intersection indicates to which extent the participation rate of the group is likely to grow. In other words, how many people will be influenced by the sequential decision-making cascade until the cascade eventually stops.

In Figure 2, the intersection of the two abovementioned lines occurs at the point *X* (40,39). The gradients of the line-segments indicate a stable equilibrium is reached. The equilibrium-state may be interpreted as an indication that sequential decision-making will influence up to 40% of the group to not report security incidents.

Many other explanations and deductions can be made from the graph but are limited to only those mentioned above due to space considerations. For a more comprehensive discussion on how behavioural threshold analysis graphs can be used and analysed, refer to the work of Growney (1983) and Granovetter (1978).

# 4 REFLECTION

## 4.1 Theoretical Implications

The arguments in this paper are of an introductory nature and attempt to explore new ideas that can help with the problem of human information security behaviour, which is often paradoxical. While no-one doubts the importance of the human factor in information security, it appears that the models used to explain it (theory of planned behaviour, protection motivation theory, etc.) have a disadvantage because they do not specifically take into account sequential decision-making and the influence of other people's decisions.

Information security behaviour is essentially a decision-making process where one must decide whether or not to perform an information security behaviour. When people work in a group setting and are aware of what other employees are doing (deciding) then the problem will be further compounded by sequential decision-making aspects of their co-workers. In order to ultimately be applied to information security behaviour, these principles for sequential decision-making will first have to be understood, and secondly be evaluated. This brings forth a new problem of *how* to understand it and *how* to evaluate it.

The principle of information cascades is presented in this article as one possible way of trying to understand information security behaviour and sequential decision-making specifically. The principles of how information cascades work as well as the four prerequisites (Section 2.1) for an information cascade fits the problem of information security behaviour (especially in a group or departmental setting where people can observe others' behaviours and decisions). Information cascades therefore provide a possible solution for understanding information security behaviour under certain circumstances.

In order to address the “how to evaluate” problem, the principles of information security behavioural threshold analysis are offered as a viable evaluation tool. Section 2.2 explained the concept of information security behavioural thresholds and indicated that there exists a parallel between information cascades and information security behavioural thresholds in terms of sequential decision-making. Section 3 then presented a practical case study on how to measure and evaluate sequential decision-making by applying information security behavioural threshold analysis.

The results indicated that sequential decision-making in a group influences the individual to follow the group example in matters of information security behaviour. The extent of an information cascade that takes place may be determined with the use of behavioural threshold analysis.

Behavioural threshold analysis may, therefore, contribute to understanding information cascades and may serve to help predict the extent to which such a cascade may influence a group's behaviour.

## 4.2 Application Challenges

Behavioural threshold analysis in itself is still under continual development and therefore it brings about its own challenges in terms of its application as a method to analyse sequential decision-making and information cascades. Some of the related risks and vulnerabilities relating to behavioural threshold analysis include, among others, the following:

-The respondents in a behavioural threshold analysis exercise need to have an intimate knowledge of the behaviour of the other group members. Due to their proximity in a group, the required level of knowledge is presumed. However, if this is not the case the results of the threshold analysis may be flawed;

-Even though the number of participants in threshold analysis is intentionally kept small, too small a number will not allow for accurate analysis;

-Due to generalisation to a greater population being disallowed, little information about the behaviour of one group becomes clear by surveying another group, e.g. performing behavioural threshold analysis for the finance department does not necessarily convey information on the IT department, for instance or about the company as a whole;

-No universal measurement instrument for behavioural threshold analysis currently exists. Even though there is continual development, these instruments may need to be customised for each application; and

-Respondents may not always be truthful in their responses to questionnaires due to a perceived correct or expected answer that the researcher would like to see. This phenomenon is called social desirability. Mechanisms to test for social desirability may be investigated to control for the occurrence thereof.

## 4.3 Contributions

The main contributions of this paper can be summarised as follows:

-As described in this paper, this research is the first to attempt to link sequential decision-making, and specifically information cascades, with information security behaviour and to show a possible explanatory relationship between the two;

-Sequential decision-making and information cascades provide a model to understand and evaluate (often paradoxical) information security behaviour;

-This study suggests a solution on how to evaluate sequential decision-making by means of an information security threshold model. This suggested solution is explained, motivated, and illustrated by presenting an investigative real-life case study; and

-By theorising on concepts like information cascades and information security thresholds, this research can potentially create new avenues for further research and enquiry which in turn might provide new insights on the problem of paradoxical information security behaviour.

# 5 CONCLUSION

This paper explored the possible influence of information cascades in security behaviour. Section 1 contextualised the research in the domain of human aspects of information security. In Section 2, the concept of sequential decision-making was presented. Two models were presented that aim to describe sequential decision-making in a group context, namely information cascades, and behavioural thresholds. These two models were shown to be mutually inclusive. An illustrative case study, to indicate how behavioural threshold analysis may be used as an instrument to evaluate information cascades and sequential decision-making was presented in Section 3. In Section 4, a reflection on the theoretical implications and practical challenges of this research is discussed, and the section concludes with a summary of the contributions of this paper.

Sequential decision-making and information cascades may contribute to how individuals determine their behaviour in terms of information security. Behavioural threshold analysis may contribute to understanding information cascades as the two approaches share many similarities and are applicable under the same circumstances. The findings of this research are still in its infancy and should therefore be understood as such. The theories and concepts that are discussed in this paper, warrant

further investigation in order to better understand the implications thereof.

## REFERENCES


Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50**,** 179-211.

Alshaikh, M., Maynard, S. B., Ahmad, A. and Chang, S. 2018. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations.

Arce, I. 2003. The weakest link revisited [information security]. *IEEE Security and Privacy*, 99**,** 72-76.

Banerjee, A. V. 1992. A simple model of herd behavior. *The quarterly journal of economics*, 107**,** 797-817.

Bikhchandani, S., Hirshleifer, D. and Welch, I. 1992. A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of political Economy*, 100**,** 992-1026.

Chesney, R. and Citron, D. K. 2018. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21*.

Easley, D. and Kleinberg, J. 2010. *Networks, crowds, and markets: Reasoning about a highly connected world*, Cambridge University Press.

Glaspie, H. W. and Karwowski, W. Human Factors in Information Security Culture: A Literature Review. In *Advances in Human Factors in Cybersecurity: International Conference on Applied Human Factors and Ergonomics (AHFE 2017)*, 2017 Los Angeles, CA, USA. Springer, 269-280.

Granovetter, M. 1978. Threshold models of collective behavior. *American Journal of Sociology*, 83**,** 1420-1443.

Growney, J. S. 1983. *I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior*, Bedford, MA, COMAP Inc.

IBM Security 2018. *IBM X-Force Threat Intelligence Index 2018: Notable security events of 2017, and a look ahead*. USA: IBM Corporation.

Kroenung, J. and Eckhardt, A. 2015. The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Information and Management*, 52**,** 611-627.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M. and Hohler, B. Employees' information security awareness and behavior: A literature review. In *46th Hawaii International Conference on System Sciences (HICSS)*, 2013. IEEE, 2978-2987.

Lineberry, S. 2007. The human element: The weakest link in information security. *Journal of Accountancy*, 204**,** 44.

Ooi, K.-B., Hew, J.-J. and Lin, B. 2018. Unfolding the privacy paradox among mobile social commerce users: a multi-mediation approach. *Behaviour and Information Technology*, 37**,** 575-595.

Pham, H., Brennan, L. and Richardson, J. Review of Behavioural Theories in Security Compliance and Research Challenge. In *Informing Science and Information Technology Education Conference, Vietnam*, 2017 Santa Rosa, CA, USA. Informing Science Institute, 65-76.

Snyman, D. P. and Kruger, H. A. Behavioural thresholds in the context of information security. In *10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 2016 Frankfurt, Germany. Plymouth University, 22-32.

Soomro, Z. A., Shah, M. H. and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36**,** 215-225.

Welch, I. 1992. Sequential sales, learning, and cascades. *The Journal of finance*, 47**,** 695-732.

Wilson, T. D. 1999. Models in information behaviour research. *Journal of documentation*, 55**,** 249-270.