



Behavioural threshold analysis: methodological and practical considerations for applications in information security

Dirk Snyman & Hennie Kruger

To cite this article: Dirk Snyman & Hennie Kruger (2019): Behavioural threshold analysis: methodological and practical considerations for applications in information security, Behaviour & Information Technology, DOI: [10.1080/0144929X.2019.1569163](https://doi.org/10.1080/0144929X.2019.1569163)

To link to this article: <https://doi.org/10.1080/0144929X.2019.1569163>



Published online: 21 Jan 2019.




Submit your article to this journal [↗](#)



View Crossmark data [↗](#)



Behavioural threshold analysis: methodological and practical considerations for applications in information security

Dirk Snyman  and Hennie Kruger

School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa

ABSTRACT

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments and methodology used to gather relevant attitude data. This paper presents an analysis of the specialised requirements for such a measurement instrument and makes methodological recommendations on the content and especially presentation of information security topics in a measurement instrument for this context. A comparison between existing methods and the specific requirements for threshold analysis is presented and serves as the main rationale for the suggested methodology. The recommended methodology and subsequent measurement instrument were implemented and experimentally tested in case studies to gauge their feasibility. Applications of behavioural threshold analysis in information security that follow the recommended methodology suggested in this article performed satisfactorily and elicits cause for further real-world experimentation.

ARTICLE HISTORY

Received 18 May 2018
Accepted 24 December 2018

KEYWORDS

Measurement instrument;
behavioural threshold
analysis; information security;
behaviour; attitude

1. Introduction

Human aspects remain an important component of information security. Measuring and quantifying the human aspect, however, remains a difficult task (Connolly et al. 2016). A new proposed approach to analyse information security behaviour based on the attitudes of individuals in an organisation, is the behavioural threshold analysis technique (Snyman and Kruger 2016). The general application of behavioural threshold analysis on group behaviour was first presented by Granovetter (1978). Forming part of a larger research project, initial exploratory studies on the application of behavioural threshold analysis in information security show that this approach may help to determine attitudes and behaviours of individuals in a group setting on specific information security topics in order to help evaluate the risk associated with these topics (Snyman and Kruger 2016, 2017a). Furthermore, behavioural threshold analysis was also determined to be helpful in the construction of information security awareness programmes and also helps gauge the level of saturation that these awareness programmes have within an organisation. The inextricable connection between attitude and behaviour was once more confirmed in the application of behavioural threshold analysis for information security topics in the earlier studies (Ifinedo 2012; Snyman and Kruger 2016,

2017a; Sommestad and Hallberg 2013). The analyses in the mentioned studies suggest solutions to the unique problems in terms of the questions that have to be asked to individuals to determine their attitude towards specific information security topics. These attitudes are used to construct a collective representation of the ultimate behavioural thresholds within an organisation for the specific topic under assessment. The exploratory studies mentioned above have been previously conducted on the application of behavioural threshold analysis in the context of information security and has determined its value as an instrument to analyse collective behaviour. What remains absent is that there has not been a specific concentration on information security focus areas and the related information security questions that have to be asked for each focus area to determine individual thresholds.

Behavioural threshold analysis presents a unique challenge and differs from conventional information security awareness research and as such has very specific needs for the type of related security questions and how these questions are presented (Snyman and Kruger 2016, 2017a). For instance, typical behavioural threshold analysis requires a mechanism to elicit individual threshold values expressed as a percentage or number of group members. Specifically, for information security

research, these threshold values are in terms of sensitive information security behaviours. The method of response available to the respondent is also a unique issue in behavioural threshold analysis. It remains to be determined whether threshold values should be answered in a direct response, or whether the thresholds should be presented as intervals with respondents indicating levels of agreement.

Question structure is another factor and includes how the question is worded, presented and set out. The sensitive nature of the questions leads to social desirability being a specific problem that needs to be kept in mind when determining which topics to include in questioning and how questions are presented. Another specific issue is asking the minimum number of questions but retaining the maximum coverage of risk types. Special attention to the questions that are asked is moreover due to the requirement that people need to be aware of other people's information security behaviour (Growney 1983). This means that only certain kinds of question can be asked and not just any of the information security questions that have been previously determined. Therefore, specific attention has to be given to questions about information security behaviour that is not conducted in secret where others will not know about the behaviour, but rather behaviour that is conducted openly where others can be aware thereof.

From the argument above, the specialised prerequisites for a specific methodology for creating a measurement instrument for behavioural threshold analysis is evident and is formalised in the following problem statement:

Due to the unique requirements of an information security threshold application, traditional information security measurement instruments are insufficient and need considerable adaptation to determine behavioural thresholds.

Existing approaches to behavioural threshold analysis have been tested in earlier work by applying them in information security (Snyman and Kruger 2017a). From the earlier work, the opportunity to improve upon the existing method became evident. This indicates that there is a definitive gap in the current state of research where this study can make a valuable contribution.

Therefore, the current research aims to answer the following research question:

Can a unique information security behavioural threshold measuring instrument be developed that will address the special nature and requirements of a behavioural threshold analysis methodology in the context of information security?

In order to guide the study to answer the research question above, it is divided into the following three sub-questions that address the unique requirements of behavioural threshold analysis in the context of information security:

- *How should sampling be conducted for behavioural threshold analysis in information security?*
- *Which aspects should be considered in terms of question design for behavioural threshold analysis in information security? and*
- *Which factors should be provided for to ensure the validity of data collection for behavioural threshold analysis in information security?*

The aim will be achieved by formulating and motivating some basic information security questions to measure attitude (and behaviour) in some common information security focus areas. Specific reference will be made to the presentation of these questions to respondents and the requirements of behavioural threshold analysis. The research that is presented in this paper specifically differs from the previous work in that the initial inquiries aimed to test the feasibility of the behavioural threshold analysis approach for information security. The approach was found to provide promising insights and now this study presents part of the process to fine-tune the methodology to contribute to its maturity. The main contribution of this research is that it provides a methodology for the construction of a measurement instrument for behavioural threshold analysis for applications in information security.

The structure of the remainder of this paper is presented as follows: In **Section II**, a cursory background is given on the human aspect in information security, as well as behavioural threshold analysis and its application in information security. In **Section III**, an overview of the most prominent forms of information security behaviour is presented. In **Section IV**, some examples of specific questions for behavioural threshold analysis are provided, while in **Section V**, case studies are presented to illustrate their use. The proposed methodology is presented in **Section VI**. Exercises that validate the proposed methodology are described in **Section VII**. Finally, in **Section VIII** a reflection on the study is presented and in **Section IX** the findings of this research are summarised and future directions for the application of behavioural threshold analysis in the context of information security are anticipated.

2. Related work

As explained in Section I, this research forms part of a series of articles in an overarching research project on behavioural threshold analysis and its application in the field of information security. As such, only a high-level overview of the related human aspects in information technology and general behavioural threshold concepts is provided in this section.

2.1. The human aspect in information technology

Human aspects in information security have been identified as one of the core aspects (alongside organisational and technical facets) that form part of the process to ensure the fidelity and protection of information systems within an organisation (Safa, Von Solms, and Fitcher 2016). For the most part, technical and organisational issues pertaining to information security have been thoroughly thought through and addressed and continue to be effectively managed in organisations (Scholl, Leiner, and Fuhrmann 2017). The human aspect, however, is still to be as successfully managed as these other core aspects. This is due to a relative ineptitude of organisations and their managing structures to identify and control the human factor, as it is a complex and ever-changing phenomenon. The human factor within an organisation is often said to be directed by the collective organisational culture that is based on the attitudes, norms and behaviours of the individuals that make up the organisation (Ashenden 2008). This is also the case with information security culture, which is driven by the same collective outlook that the individuals in an organisation express towards information security policies and practices (Da Veiga and Martins 2017; Dhillon, Syed, and Pedron 2016). Their communal attitude towards policies and other security measures often determines whether these controls can be effectively implemented to protect the information assets of the organisation or could, on the other hand, cause them to fail. Attitude is a common antecedent for behaviour (Ajzen 1991; Fazio 1990) and as such the topic of attitudes in information security has received much attention in recent studies (Cuganesan, Steele, and Hart 2018; Ifinedo 2012; Nguyen and Kim 2017; Snyman and Kruger 2016; Sommestad et al. 2014). Attitude towards compliance with information security policies should determine the eventual actions that the individuals in a group perform, either following or disregarding these policies. The corroboration of the link between attitude and behaviour has been formalised by the expression thereof in terms of theoretical models.

One of the better-known models is the theory of planned behaviour, first described by Ajzen (1991). This model shows the influence that the attitude towards behaviour has on an individual's intentions, which is ultimately expressed in his/her behaviour. The theory of planned behaviour has been used to contextualise many studies in information security behaviours and attitudes (Al-Omari, El-Gayar, and Deokar 2012; Ifinedo 2012; Pattinson et al. 2016; Snyman and Kruger 2017a; Sommestad and Hallberg 2013). Another influential model for attitude and behaviour in information security is the knowledge, attitude and behaviour model (Kaur and Mustafa 2013; Kruger and Kearney 2006; Parsons et al. 2014). An example of this model would be the knowledge that a person has about information security policies influencing his/her attitude about information security topics, which in turn determines the actions (behaviour) that the person takes when confronted with information security challenges. Measuring attitude (linked to behaviour) in terms of information security remains a challenging endeavour. Two of the more common approaches to measuring attitudes is by using self-reporting questionnaires, such as the HAISQ (Parsons et al. 2014; Parsons et al. 2017) and the use of repertory grid technique interviews (Pattinson et al. 2016; Pattinson et al. 2015).

2.2. Behavioural threshold analysis

The idea of behavioural threshold analysis stems from the initial model presented by Granovetter (1978) in which the collective behaviour of a group of people is said to be based on the individual's attitude towards participating in a group activity, given his/her awareness of the proportion of others in the group that participate in the activity. The attitude is said to be expressed in terms of the number of members in the group that have to participate in a certain action before the individual will be inclined to also partake. This is said to be the individual's threshold for participation (Granovetter 1978). The behavioural threshold model can theoretically be applied to any situation where a group is confronted with a contrasting decision, for instance the spreading of a rumour. If a rumour is heard by an individual X from one person in a group, he/she might discard the information as being untruthful due to an inherent level of naiveté or lack of evidence. Contrarily, if the rumour is heard from enough other persons in the group (i.e. individual X's threshold of participants in spreading the rumour is exceeded), individual X will accept the rumour and also start spreading it due to the perceived credibility the number of members of the group that spread it add to the rumour.

Group behaviour in information security can also be expressed as two contrasting courses of action, i.e. a binary decision (Snyman and Kruger 2017a) and therefore presents the opportunity to implement behavioural threshold analysis. Based on the collective information security activities of the members in a group, and the individual's attitude (threshold level) towards also participating in those activities, a prediction of the eventual information security actions of the group can be made. This prediction is based on the analysis of the individual thresholds according to the behavioural threshold analysis model. The analysis, using the model, is only possible when the individual thresholds for information security actions of the members of a group are known (Granovetter 1978). As such, a mechanism of eliciting threshold information from the members is needed. The aforementioned threshold value of an individual is directly determined by the individual's attitude towards participation in the group action.

Growney (1983) suggests a questionnaire as the instrument for gathering the individual thresholds from a group for any group activity situation. The questionnaire is structured in a very specific way where respondents choose their preferred outcomes and nominate their own threshold values for participation. The questionnaire was used in an earlier, related study (Snyman and Kruger 2016) to test the application of the behavioural threshold model for information security. Figure 1 shows an example information security question similar to the one, which was presented to respondents in Snyman and Kruger (2016) in the format, which was suggested by Growney (1983).

The respondents were tasked with nominating their threshold value for sharing their passwords with others. The threshold was expressed as a percentage of group members that would need to share their passwords with others before the respondent would also do so. The results

obtained for the initial experiments in Snyman and Kruger (2016) did not follow the expected trends seen from literature. This indicated that there are some problems with the measurement instrument in its current form.

In an attempt to improve the behavioural threshold approach for information security, the results from Snyman and Kruger (2016) were critically analysed in another related study (Snyman and Kruger 2017b) and some key issues were identified that need to be addressed to help improve the feasibility of the behavioural threshold analysis approach in this context. Snyman and Kruger (2017b) investigated a novel alternative to the questionnaire as the measurement instrument for information security thresholds by employing an optical polling method for data collection. The suggested optical polling method could address some of the issues, but under certain circumstances, it would remain beneficial to employ a questionnaire as the instrument of choice (for instance different geographical locales, etc.). Issues that were identified that are specific to questionnaires on behavioural thresholds in information security and are relevant to this research are reiterated here for context and motivation for the aim of this study. Data collection for behavioural threshold analysis requires a unique method of questioning. The initial questionnaire wording and structuring created confusion, which led to respondents misunderstanding the question and answering incorrectly, possibly due to the following causes:

- For behavioural threshold analysis (especially when applied to information security), the topics that are used in questioning need to be suitable and well thought out. The choice of the topic (password security) that was used previously might have failed to yield the expected results due to the familiarity that respondents could have had with recommended practices for the topic;

Questionnaire	
1. Choose one of the following outcomes that is preferable:	
a. A situation where no student will share his/her password with any other student.	
–OR–	
b. A situation where every student is free to share his/her password with any other student.	
2. Regardless of the outcome selected above, respond to one of the following statements:	
a. I will never share my password with another student.	
–OR–	
b. I will share my password with another student when at least x percent of students shares their passwords. (nominate a value for x)	

Figure 1. Behavioural threshold questionnaire adapted from Growney (1983).

- Due to the sensitive nature of the typical information security topic, respondents tend to either over-, or understate their attitudes towards the behaviour of others who deal with these subjects. They wish to portray a version of themselves that is more socially acceptable than their actual self. This tendency is called social desirability (Fisher 1993) and it is especially important in a setting where the influence of members in a group on each other is expected. A group setting in itself is essentially a social situation, regardless of whether the group is an organisational or friendly one. Individuals' perceived social identities and group membership determine that they would be very susceptible to social desirability, presenting themselves as they would want to be perceived in an attempt to fit in with the group (Tanis and Postmes 2005).
- Behavioural threshold analysis in the context of information security is currently unknown to the conventional respondent. With this in mind, traditional questionnaires might not convey enough background information on exactly what is expected from respondents. In addition, the structure of the questionnaire might not provide enough guidance for a respondent to reply confidently in the expected fashion. Mechanisms would need to be employed to restructure the approach and guide a respondent through the process and in doing so prevent responses that do not fit the expected patterns; and finally
- The nature of the topic on which the questions are based should be such that the behaviour of an individual is known to other members of the group. Behavioural threshold analysis is reliant thereon as an individual's threshold is based on the behaviour of the group around him/her and if the individual is not aware of other's behaviour he/she cannot be influenced and cannot express an inclination to follow their example. This implies that any behaviour that is not practised in the open, or at least practised without specifically being hidden by the members in the group, is not suitable as a topic for behavioural threshold analysis (Granovetter 1978). Most likely behaviour with specifically harmful intentions would be done in secret. By contrast, behaviour that is not known to the perpetrator to be detrimental may not be hidden due to no perceived wrongdoing or threat. This has the implication that not all information security questions from literature can be used without ensuring the question conforms to this specification. This does not preclude the use of existing questions, but simply that special consideration should be given to the underlying behaviour about which the question asks.

The effect of the social desirability bias, albeit in a general sense, is seen in the work of Dahlgren and Hansen (2015) in the tourism sector. They report that respondents gave biased answers when asked questions about their opinion of a country when they perceive that the interviewer has the same nationality as said country. The bias is attributed to respondents *not wanting to offend* the interviewer. If the country and nationality are not the same, they tend to be more honest because their social perception dictates that the interviewer will not feel offended in this instance. See also the works of Van de Mortel (2008) on social desirability in health research, and Dodou and De Winter (2014) on social desirability in online, offline and paper surveys.

Similarly, in terms of behavioural thresholds, social desirability is expected to lead to *lower* thresholds for *actual* participation, i.e. the individual should easily comply with the group even if the behaviour is undesirable. This would be due to the intrinsic pressure experienced by the individual to *fit in with* or *not offend* the group. Consequently, the individual *does as the group does* in terms of its information security behaviour. On the other hand, when *asked* about participating in undesirable behaviour, the individual is likely to report a *high* threshold indicating he/she would not be swayed by the group. The individual knows that *doing as the group is doing*, in terms of bad practices, is not what is expected of him/her. They report that the individual will not easily follow the example as to *not offend* or *conform to the expectations* of whosoever sees his/her responses. This paradox of actual versus reported behaviour is problematic for the interpretation of threshold values. Mechanisms to control for the effect of social desirability should be investigated;

In summary, these issues mentioned above indicate the direction for the investigation that is presented in this paper. It furthermore serves to reaffirm the premise that the measurement instrument cannot follow the existing trends and the underlying methodology will have to differ in most aspects. The traditional approaches need to be revisited in order to address these issues to fit the unique requirements for behavioural threshold analysis. In the following section, how information security behaviour is currently classified and implemented in information security research and how behavioural threshold analysis questions can be determined are described. Special attention is given to the requirements for behavioural threshold analysis, namely what topics are suitable for behavioural threshold analysis in information security and how the questions on a

questionnaire should be presented to obtain trustworthy results. Attention is given to the overtness of the behaviour and whether the behaviour would typically be performed with the explicit knowledge of others.

3. Information security behaviours

In order to ascertain suitable information security topics for behavioural threshold analysis, it is imperative to look at information security topics and questions in general and how they are expressed and handled in literature. Specific attention is given to whether the specific behaviours from literature conform to the specifications as set out above.

Pattinson et al. (2016) define information security behaviour as simply: ‘... the full spectrum of behaviours [actions] by people who make significant use of computers as part of their job.’ Based on an earlier study by Pattinson and Anderson (2007), these behaviours are categorised into three discrete types of information security behaviour that are ‘deliberate risk-averse behaviours’, ‘Naïve and accidental behaviours’, and ‘Deliberate risk-inclined behaviours’. Some examples of these behaviours are also presented by Pattinson and Anderson (2007) and include: Always logging off when computer is unattended (deliberate risk-averse), opening unsolicited e-mail attachments (naïve and accidental), and writing and disseminating malicious programmes (deliberate risk-inclined).

This classification is based on a mapping of a larger taxonomy for information security behaviours that was introduced by Stanton et al. (2005). Their taxonomy was constructed by interviewing information security experts about their experience with positive and negative information security behaviours within different organisations. After refactoring the original behaviours by merging similar behaviours into groups, a six-element taxonomy was constructed, which categorises information security behaviours on two features, namely intent and skill. Intent looks towards the eventual outcome that was envisioned by the person performing the specific behaviour, i.e. a positive or negative eventuality for the organisation. Skill refers to the level of technical proficiency that is required to execute the behaviours. Each behaviour is then expressed with a rating of one (low) to five (high) for both skill and intention. Interestingly it was noted that the higher the intentionality of the behaviour, the higher the required skill level for the behaviour became (Stanton et al. 2005).

The categories for information security behaviour by Pattinson et al. (2016), that were referred to earlier, were mapped from the taxonomy suggested by Stanton et al. (2005). They identify ‘naïve and accidental

behaviours’ as their category of interest for a comparison of data collection methods for information security attitudes. This provides the direction for using the same kind of ‘naïve and accidental behaviours’ as the basis for behaviour threshold analysis. In comparison, the other two categories are either mostly unsuited for this research (‘deliberate risk-inclined behaviours’) or still indicated for inclusion in future work (‘deliberate risk-averse behaviour’). ‘Deliberate risk-inclined behaviours’ are behaviours that, for the most part, require a high level of skill. Furthermore, seeing that these behaviours are deliberate, they are known by the offender to be behaviour that is not acceptable as good information security practice. Such behaviours are therefore most likely done in secret and those that practise them are very unlikely to let others in their organisation find out what they are doing, let alone admit to the behaviour on a research survey. Recall that behavioural threshold analysis requires the members of a group to be aware of the actions of others for the model to be applied. Therefore, ‘deliberate risk-inclined behaviours’ are excluded from this research. The other end of the spectrum involves ‘deliberate risk-averse behaviours’, which are behaviours that are considered beneficial to the overall well-being of an organisation’s information security and culture. These behaviours will likely be practised overtly, without the individual wanting to hide his/her actions. Other members of the specific group would therefore be aware of this behaviour and the behaviour should also have an influence on their collective behaviour. Inclusion of risk-averse behaviours in behavioural threshold analysis falls beyond the scope of this paper but is planned for inclusion at a later stage.

Furthermore, ‘deliberate’ information security behaviours are typically covered by information security policies, which would make their analyses a question of policy compliance (Al-Omari, El-Gayar, and Deokar 2012; Ifinedo 2012; Vance and Siponen 2012). For this specific study, the focus is on ‘naïve and accidental behaviours’. By implication, the naïve individual may not have knowledge of existing policies that exist to govern his/her behaviour and cannot therefore comply with guidelines that the individual does not know exist. Furthermore, even if the individual does have knowledge of policies he/she may still be deceived due to his/her naiveté regarding, for instance phishing attacks. Accidental behaviour may also be performed by individuals who are well versed in policy matters. A seemingly harmless action might cause a security vulnerability by accident. Retrospective to behavioural threshold analysis for information security topics, policies may be inferred from the results specifically to guide future behaviour in conjunction with security awareness programmes. This,

however, falls outside the scope of the current research and is indicated as possible future work.

When an individual is unaware (i.e. naïve) that his/her behaviour is unwanted, that individual will most likely exhibit 'naïve and accidental behaviours' without much thought to consequences of what should happen if the behaviour is known. Members of the group should therefore be aware of each other's naïve and accidental actions. These behaviours are also of such a nature that they could be harmful to an organisation's information security and fidelity (Pattinson et al. 2016). A relatively low skill level is required for behaviour that falls into this category, which means that most individuals in a group should be able to perform these actions. Furthermore, Parsons et al. (2014, 2017) also used naïve and accidental behaviour as the basis for the development of the HAIS-Q (Humans Aspects of Information Security Questionnaire). The HAIS-Q is used as an aid in determining specific topics for behavioural threshold analysis in information security, with the difference that the topics are expressed in a manner that is conducive to the unique requirements set out for threshold analysis. In the following section, example questions for behavioural threshold analysis when it is applied in the context of information security are presented.

4. Example information security questions for behavioural threshold analysis

An annual survey of international information security threats is conducted by PricewaterhouseCoopers to inform business leaders of information security risks. In the report 'The Global State of Information Security Survey' (PWC 2017) it is stated that there is an awareness among company executives of the possible consequences of cyberattacks. Nevertheless, almost half (48%) of the companies which were surveyed do not have structures in place to address general information security awareness among employees. Furthermore, 54% of these companies do not have incident-response strategies. While it is acknowledged that these shortcomings should first and foremost be addressed at an executive level, there is a resulting gap in the typical employee's awareness and general information security hygiene. This lack of awareness and skills is sure to have an influence on their eventual information security behaviour.

The Human Aspects of Information Security Questionnaire (HAIS-Q) is a measurement instrument, developed by Parsons et al. (2014), to quantify the information security weaknesses that are perpetuated by humans. The instrument was tested for validity and reliability and can be considered as one of the better established and mature instruments for assessing security awareness. The

modular nature of the HAIS-Q allows the instrument to be adapted for testing awareness for specific aspects of information security that are of interest (Parsons et al. 2017). To this end, the HAIS-Q is divided into information security focus areas, each with a specific set of related behaviours. With the specifics of behavioural threshold analysis in mind, the HAIS-Q was used as a basis for determining a series of questions for the construction of a measurement instrument specifically for the application of threshold analysis for information security behaviour. These behaviours were chosen to also be representative of typical problematic information security areas that are identified in information security audits and surveys as mentioned above.

Table 1 shows example information security questions for behavioural threshold analysis, based on the focus areas and associated security behaviours ('naïve and accidental'), which were identified from the HAIS-Q. The questions were formulated in the style required for behavioural threshold analysis and were subsequently included in case studies on the implementation of behavioural threshold analysis in information security.

The HAIS-Q describes more focus areas with themes, such as mobile devices and information handling (Parsons et al. 2017) that are not included in Table 1. After due consideration of the specific contexts in which the case studies and further validation studies were to be conducted, only the five focus areas in Table 1 were selected for inclusion in the experimental phases of this research. It should be noted, however, that depending on the requirements of the specific behavioural threshold study, one might include more of the focus areas and include multiple associated

Table 1. Example questions based on focus areas and behaviours from HAIS-Q.

Focus area	Information security behavioural threshold question
1. Password management	How inclined would you be to also share passwords, given the percentage of colleagues who share their passwords?
2. Social media use	How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who 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 colleagues who 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 colleagues who regularly access dubious websites from devices connected to your company network?
5. E-mail use	How inclined would you be to also open any unfamiliar email attachments, given the percentage of colleagues who normally open any unfamiliar email attachments?

questions for each focus area. Caution should be exercised when deciding on adding multiple focus areas or questions in order not to overburden the respondents with lengthy questionnaires that take excessive time to complete. The number of responses that are required per question adds significantly to the burden that is placed on the respondent. Traditional questionnaires employ multiple questions to test one facet of interest (for example, incident reporting) in order to address consistency in the questionnaire (Sekaran and Bougie 2010). Once again, the unique requirements for behavioural threshold analysis necessitate a divergent approach. The model allows for only one question per facet that is to be tested.

The wording for the questions is based on the requirements for behavioural threshold analysis. In this case, a respondent indicates his/her level of inclination to join in the corresponding behaviour when different percentages of the group are participating in the behaviour (i.e. the threshold for participation). The inclination is expressed on a four-point Likert scale, and the corresponding percentage of participants in the group is presented in intervals of 10%. Table 2 presents an example of how one of these questions would be presented in its entirety. Each question is presented as a grid of possible thresholds and respondents would have to nominate a response for each threshold interval resulting in ten responses per question. The suggested layout draws from the recommendations of Pattinson et al. (2016) that a combination of repertory grid interviews and traditional questionnaires is advisable for information security behaviour research. The responses for the threshold intervals are required in order to conduct the mathematical analysis and prediction of the group behaviour. It is therefore recommended that a balance be found between the coverage of topics and the number of questions asked.

Table 2. Example of a complete behavioural threshold question.

Percentage of colleagues who spend excessive work time on social media	How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who spend excessive work time on social media?			
	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

In Section II, it was remarked that social desirability is a problem when using questionnaires for data collection, with specific implications for behavioural threshold analysis. Mechanisms for measuring the levels of social desirability that a respondent exhibits date back some time. Most influential is the work of Crowne and Marlowe (1964) who developed a fully-fledged instrument to measure whether a respondent is answering truthfully or whether social desirability has tainted his/her response. The Marlowe-Crowne social desirability scale is a 33-item questionnaire that presents a respondent with statements that could be deemed socially positive and others that are socially negative. Respondents are asked to respond only whether the statement is true, or false, pertaining to them personally. A set of expected responses to the questions is predetermined, coded as true for 18 of the scenarios and 15 for false. The expected responses are based on whether a truthful respondent would answer true to statements that would place him/her in a bad light socially. The responses are scored, and the level of social desirability can be determined as either high or low. Due to the number of questions that are included in the Marlowe-Crowne scale, shortened versions of the scale have been proposed (Reynolds 1982) and later validated (Ray 1984) to convey a reliable account of a respondent's level of social desirability. The short social desirability scale, which was validated by Ray (1984) consists of only eight questions answered by only Yes, No or Unsure. Each of these responses is coded and scored based on the specific question. These eight questions were included in the subsequent case studies, supplementing the five information security questions (see Appendix A).

The premise, at least for behavioural threshold analysis, is that a respondent who exhibits high levels of social desirability would nominate threshold values that are higher than their actual thresholds, e.g. that he/she would share his/her password when 31–40% of others in their group share their passwords. The truth is that a respondent may in fact share his/her password when only 11–20% of others in the group do so. The thresholds for a respondent who shows social desirability could conceivably be adapted downwards by a conservative margin (e.g. one threshold interval or 10%). This should lead to representations of the personal thresholds within a group being more trustworthy and allow the eventual collective behaviour of the group to be predicted with better accuracy.

From the discussion in this section, it becomes evident that the proposed questionnaire differs considerably from the typical information security behaviour questionnaires. Furthermore, the analysis and interpretation of the responses are also treated differently in that a

specialised mathematical analysis of the results is performed rather than the traditional statistical methods that are commonly used in the analysis of traditional questionnaires. In Section V, two illustrative case studies where these questions were implemented, and provision was made for the occurrence of social desirability are described.

5. Illustrative case studies

Two case studies were completed to validate the choice of behavioural threshold analysis questions for group behaviour in information security, as well as the method for presenting the questions to respondents. Before the case studies are presented, a note on the sample sizes that are reported for each of the case studies: As mentioned earlier in Sections I, II, and III, the behavioural threshold analysis approach requires individuals to be aware of the behaviour of the other members of the group (Growney 1983). It stands to reason that an employee will only be aware of the behaviour of individuals that he/she comes into contact with on a regular basis, i.e. another person in the same organisational group or department. On the other hand, global tendencies in information security behaviour might be propagated through media or other public information sources, which in turn creates an awareness that transgresses organisational boundaries. Analysing these large-scale trends falls outside the scope of the model. In this instance, global trends are overlooked in favour of more immediate behaviours in an organisational setting. Therefore, in order to judge the immediate group influence and behaviour accurately, only the relevant group members should be included in the exercise. When including members from outside the individual's frame of reference in terms of behavioural examples, the model might become skewed and the results less reliable. The required awareness therefore dictates that the sample sizes are specifically kept small. This is another example of the uniqueness of the behavioural threshold analysis model and how it differs substantially from the other established approaches to measure information security behaviour.

5.1. Case study 1 (Snyman and Kruger 2016)

The first case study was conducted with a group of 22 first-year engineering students at a South African university. The information security question that was used in this instance was based on password management and was presented in the format of Figure 1:

I will share my password with another student when at least x percent of students share their passwords (nominate a value for x). (Focus area: Password management)

The information security question along with some questions on biographic information was distributed to the group via Google Forms. The structure of the question was presented in such a manner that the respondent had to nominate a value for x by typing in the relevant percentage value. In this case study no questions on social desirability were asked and no adjustment of the nominated thresholds was done. The case study was intended to be an initial test to see how a skeleton questionnaire would fare for behavioural threshold analysis. After the cumulative results for the nominated behavioural thresholds were calculated, the resulting graph in Figure 2 was obtained.

The graph represents an aggregate of the thresholds of the individuals, given the percentage of group members who share their passwords. For instance, the point (20,10) indicates that 10% of individuals will share their passwords when 20% of the group do so. The graph did not follow the expected trends. The expectation was that individuals would have low thresholds for password sharing, i.e. they would be willing. The group of students was observed throughout a semester during practical programming classes in a shared computer laboratory. They need a network username and password to access the workstations in this environment. Password sharing was often observed to occur when one student's credentials have expired or were forgotten. Resetting the expired credentials would entail a visit to an IT helpdesk in another building some distance away. So, in order to save time another student would simply supply their credentials so that a classmate is able to access a workstation to complete the assignment that is due by the end of the practical session.

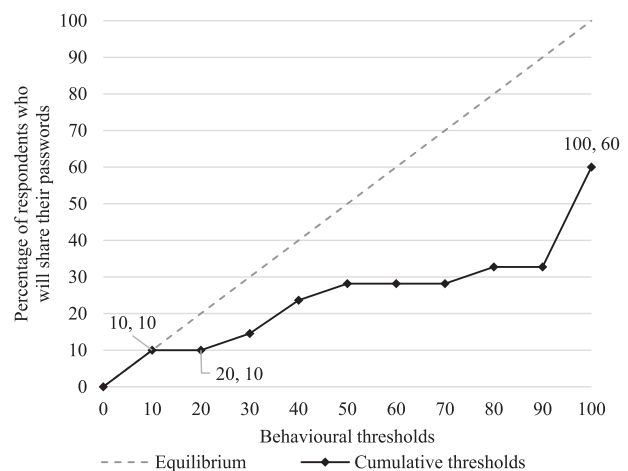


Figure 2. Behavioural threshold analysis for case study 1 (Focus area: Password management).

The network credentials in question are also used for authentication with other network resources, such as printers, network storage, e-mail server, learning management system, financial and academic statements, etc. If another user is privy to one's credentials, he/she can therefore access any and all resources for which the credentials are authorised. Whether the risks are known and understood by the students is not clear, but through the above-mentioned observation, it was known that the group was quite comfortable with sharing its passwords among the members and it is a practice that was done on a regular basis (even though the practice is not recommended).

The notion of password sharing among students is supported by Shay et al. (2010), who conducted research on behaviour and attitudes relating to passwords. They found that 33% of the undergraduate students that they surveyed were engaging in password-sharing behaviour. Another, more recent, study on password behaviour, reports an even higher password-sharing rate of between 50–60% for a non-homogenous sample in a South African context (Butler and Butler 2018). Since the case study was performed in a South African context, this result should also be indicative of what could be expected in terms of the results for password sharing from case study 1.

The two main reasons that were identified for the unexpected results were, either the respondents do not understand the question and how to answer it correctly, or respondents chose to misrepresent their actions by not answering the question truthfully because they are aware that password sharing is frowned upon, i.e. they display high levels of social desirability. A combination of social desirability and misinterpretation was thought to be the most likely cause for the results not conforming to the expected standard. For a detailed interpretation of the graph and related recommendations, see Snyman and Kruger (2016). Taking its direction from the lessons learnt in the first case study, a second case study was completed as described in the following sub-section below.

5.2. Case study 2

A second case study was conducted as part of the current study to improve upon the two issues that were identified from the first case study, i.e. question format and social desirability. Another question was selected and a new online questionnaire (once more facilitated through Google Forms) was constructed and a more guided approach to threshold selection was followed based on the recommendations of this research. The questionnaire was completed by 16 staff members at a university within a departmental setting. The layout and the question in Table 2 was used, i.e. a grid layout (inspired from that of a repertory grid) where a respondent would have to

rank his/her level of inclination for participation in the behaviour that was described in the question, given the percentage of others that perform the behaviour. The question is reiterated below and is an example of social media use:

How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who spend excessive work time on social media? (Focus area: Social media use).

Even though the question seems to be about work time management, there are underlying information security risks associated with social media use that are addressed (e.g. sharing of sensitive company information). The information security question was supplemented with the eight social desirability questions as described in Section IV. The inclination level mentioned above was tested for each of the threshold intervals. For this case study, it was decided that the first level of inclination that represents a willingness to participate in the action would be used to determine the threshold value for the individual respondent, i.e. answering at least that he/she was 'Somewhat willing' to participate in the behaviour. Helfinstein, Mumford, and Poldrack (2015) argue that the influence of group behaviour on an individual is great enough that that individual would follow group actions based only on the perception that others in the group are doing it, without much proof that they indeed perform the actions. This colloquially coined *lemming effect*¹ may be strong enough to cause the individual to act in a manner that is contrary to his/her own convictions (Helfinstein, Mumford, and Poldrack 2015). The results obtained for the second case study are presented in Figure 3. The graph closely follows the expected trends from literature.

Initially, around 31% of individuals expressed relatively low thresholds to use excessive work time for social

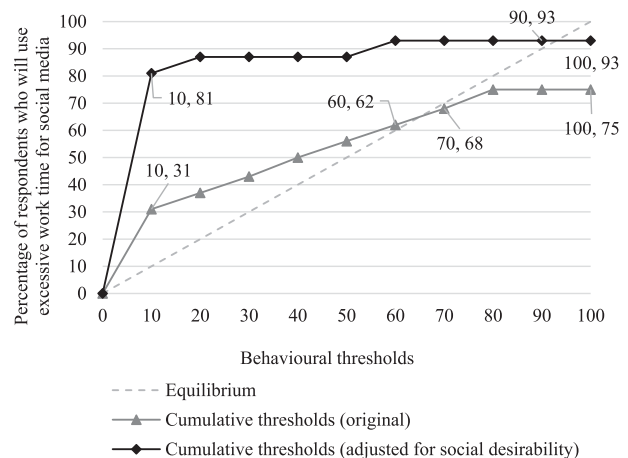


Figure 3. Behavioural threshold analysis for case study 2 (Focus area: Social media use).

media activities when others also do so (see cumulative thresholds – original – trend line in Figure 3). The graph of the cumulative thresholds indicates that excessive social media use is likely to grow until between 62% and 68% of the group members participate. The behavioural equilibrium is reached at this stage with the participation trend being stable against increase and stable against decrease (the gradient (m) of the line segments both sides of the equilibrium intersection is less than 1). Without any external influence, the number of participants should remain unchanged. When taking into account the influence of social desirability and adjusting the reported thresholds as recommended in Section IV (see Appendix A), the second trend line indicates that the initial 31% of individuals with low thresholds for participation should actually be closer to just over 80% (see cumulative thresholds – adjusted for social desirability – in Figure 3). The eventual equilibrium ($m = 0$) is established at over 90% of the group participating after the adjustment for social desirability. This indicates that the inclusion of the social desirability questions helps establish a better view of the actual behaviour exhibited by the group, rather than the reported behaviour. When factoring in social desirability the outcome is not necessarily concrete and caution should be taken when interpreting the results. The actual thresholds most probably lie between these two extremes.

The threshold results for the group show that the individuals have low thresholds for participation in the behaviour of social media use. A low threshold indicates that the individuals are easily influenced to join others in their behaviour. The outcome might be indicative that the level of security awareness of the individuals is not sufficient, or that they are coerced into demonstrating behaviour that is contrary to their better knowledge. In the following section, recommendations for the construction of a measurement instrument are presented after which case studies that validate the recommendations are shown.

6. Proposed methodology

As mentioned earlier, threshold analysis for information security behaviour poses unique challenges in its execution, as this approach does not conform to the traditional information security behaviour research expectations. The two aforementioned case studies are a practical confirmation thereof. Therefore, the aim in this section is to provide methodological recommendations for the construction of a specialised measurement instrument. The limitations of the proposed methodology are discussed. This section concludes with a reflection on the three research sub-questions from Section I.

6.1. Recommendations for measurement instrument

The overview of information security behaviours (Section III) and related questions (Section VI), in combination with the case studies that were presented in Section V form the basis for a set of recommended practices for the construction of measurement instruments for threshold analysis. Three main groups of recommendations are identified. They are based on themes that are commonly of importance when constructing traditional measurement instruments, namely sampling, question design, and validation. The recommendations are presented in Table 3.

The methodological recommendations as set out above were subsequently implemented in a further experimental case study to analyse the performance of the suggested measurement instrument. The validation case study is presented in Section VII. The following sub-section presents a discussion on the limitations of the methodology as well as the possible threats to its validity.

6.2. Limitations and threats to validity

The suggested methodology and measurement instrument was designed with the specific, unique requirements of behavioural threshold analysis in mind. In order to meet the requirements, the approaches that are common with traditional measurement instruments had to be either adapted or replaced by other approaches to follow these specifications. By tailoring the methodology according to these requirements, it is only natural that certain limitations are introduced. Furthermore, the rationale for the methodologies that are commonly used for surveys by means of questionnaires have been applied for quite some time. Consequently, they have matured and are used throughout a number of different applications (Redmiles et al. 2017; Sekaran and Bougie 2010). Along with this maturity comes an expected level of validity and reliability. This section is therefore a discussion of the possible limitations of the methodology and the threats to its validity that may exist. The limitations and validity threats are once more discussed in terms of the research sub-questions of *Sampling*, *Question design*, and *Validation*.

Sampling – The sample sizes for behavioural threshold analysis are specifically kept small as described in Table 3. However, when the sample becomes too small (i.e. less than 10 individuals) a meaningful analysis of behavioural thresholds becomes problematic. Due to the limitation of the sample sizes, no generalisation of the results to a greater population is possible. If a greater population

Table 3. Recommendations for an information security behavioural threshold analysis measurement instrument.

		Traditional measurement instruments (Pattinson et al. 2016; Redmiles et al. 2017; Sekaran and Bougie 2010)	Suggested information security behavioural threshold analysis measurement instrument	Rationale for methodological suggestions
Sampling	Sample sizes	Large	Small	Respondents need to be aware of the behaviour of others in their group (Growney 1983). Sample size should be limited to reflect this awareness, i.e. limited to organisational boundaries, such as departments. Where departments are large, i.e. extends across multiple office spaces or geographic locations, smaller groups where the members have a direct day-to-day influence on each other should be considered.
	Sampling methods	Probability sampling	Nonprobability sampling – Purposive	Purposive sampling refers to targeting specific groups of people with a very specific knowledge (Sekaran and Bougie 2010). Given the requirements of behaviour awareness of other group members, purposive sampling is recommended for behavioural threshold analysis.
	Generalisation	Generalise results to greater population.	No generalisation of results to greater population.	Information security behavioural threshold analysis in this context is not concerned with generalising findings. The analysis is limited to the group that is surveyed.
Question design	Question format	Self-reporting questionnaire or repertory grid interviews	Combination format (questionnaire and repertory grid)	In contrast to the traditional split between self-reporting questionnaires and repertory grid interviews (Pattinson et al. 2016), a combination method is suggested. Where applicable, optical polling provides a good middle ground between the approaches with good results for behavioural threshold analysis (Snyman and Kruger 2017b).
	Question topics	Generic	Specific	For behavioural threshold analysis, especially in terms of information security, the choice of topic is of cardinal importance. Questions should concentrate on specific, predetermined focus areas and should not attempt to cover all security focus areas through a general approach. The sensitive nature of questions may lead to social desirability.
	Number of questions	May have many questions to one aspect	One question to one aspect	Traditionally, multiple questions are employed in questionnaires to examine one aspect of interest. The threshold analysis model allows for only one question per aspect (Snyman, Kruger, and Kearney 2017).
	Response scales	Uneven Likert scales with five or more items recommended	Four-item (even) Likert scale	Common practice is to allow a respondent a neutral response by using uneven Likert scales (Redmiles et al. 2017; Sekaran and Bougie 2010). Given the binary nature of behavioural threshold analysis, an even Likert scale reflects this binary decision and ensures a measurable threshold. Using an even Likert scale is also a requirement for using novel media for collecting responses, such as optical polling (Snyman and Kruger 2017b), where only four possible responses are allowed.
Validation	Social desirability	Present, but may have limited effect	Needs to be specifically controlled for	Questions on information security behaviour are sensitive by nature (Redmiles et al. 2017). Sensitivity in questions often leads to 'acceptable', rather than 'accurate', responses (Dahlgren and Hansen 2015).
	Experimental controls	Reliability and validity based on statistical metrics	Face validity and iterative testing	Face validity (also known as expert reviewing) is the process whereby the measurement instrument is evaluated for validity by experts in the specific area of investigation rather than with statistical metrics (Bolarinwa 2015; Redmiles et al. 2017). This is commonly used during developmental phases of measurement instruments. The novelty of the suggested measurement instrument necessitates iterative implementation and critical review by the researcher. The specific nature of the proposed measurement instrument disallows the commonly used metrics for determining reliability and validity. This is because the instrument is inspired by a repertory grid approach and due to the unique responses that the instrument elicits.

needs to be surveyed, the threshold analysis instrument should repeatedly be administered to different groupings within the population that meet the requirements as set out in Table 3 until the desired coverage of the population is reached.

Purposive sampling is recommended as the sampling method for behavioural threshold analysis. This sampling method requires the target group to have a specific knowledge. For behavioural threshold analysis, this required knowledge is presumed to be about the security behaviour of others. Should the expected level of knowledge not be present in the group, this will impact negatively on the validity of the results that were obtained for the behavioural threshold analysis experiment.

Question design – On the theme of question format (from Table 3), optical polling is suggested as a middle ground between common self-reporting questionnaires and repertory grid interviews. Using optical polling to present a question and facilitate response collection requires all respondents to simultaneously be present in a room. This introduces logistical issues such as scheduling, geographical locations, etc. Such logistical difficulties complicate, and in some cases even prohibit, the use of optical polling. When optical polling is not a viable option, self-reporting (online) questionnaires are therefore used which introduces the known limitations thereof to the application of behavioural threshold analysis in information security.

Specific care should be given to selecting appropriate information security focus areas and question formulation. Even when a focus area is correctly identified, having the wrong question formulation can elicit responses that do not convey the expected information about the specific focus area. Such responses have a negative impact on the validity of the results that are obtained.

In Table 3, the use of a four-item Likert scale for response scales is suggested. Using this scale might not provide enough granularity should a more in-depth analysis of the responses be needed. Furthermore, respondents may become fatigued when confronted with many Likert scale questions (i.e. ten responses for each question as presented in Table 2). Fatigue in respondents typically leads to non-completion of questionnaires as well as lower response rates (Porter, Whitcomb, and Weitzer 2004). Respondents have also been noted to randomly select responses or complete patterns with the Likert scales. Respondent fatigue impacts negatively on the reliability of the data obtained with the measurement instrument.

Validation – Table 3 makes reference to the sensitive nature of survey topics relating to information security behaviour. This leads to social desirability, i.e. untruthful answers to survey questions. If the effects of social desirability are not controlled for, the validity of the data

becomes uncertain. The mechanism to measure, and correct for, social desirability that is suggested for behavioural threshold analysis is presented in Appendix A. Special care should be exercised when adapting survey responses based on social desirability scores. Under-correcting, over-correcting, or not correcting responses will once more lead to questionable data for behavioural threshold analysis.

As stated in Table 3, the measurement instrument cannot be tested for reliability and validity using the statistical metrics that are commonly used with regular questionnaires. The instrument's validity is based on iterative testing and expert reviewing. Face validity testing depends solely on the expert reviewer. This limits the use of the measurement instrument to use by researchers who are well versed in the subtleties of behavioural threshold analysis and information security or requires the involvement of a reviewer who possesses the relevant expertise. If the researcher or reviewer is not impartial or is not seasoned enough to reliably complete a face validity review, the resulting measurement instrument can be biased or may not measure behavioural thresholds correctly.

6.3. Summary of methodology

To summarise this section, a brief overview of the methodological and practical value of the proposed methodology and its performance during experimentation is presented in terms of the main themes from Table 3. These themes are *Sampling*, *Question design*, and *Validation* and directly relate to the three research sub-questions from Section I. The themes, and where they fit into the overall behavioural threshold methodology are presented schematically in Figure 4. The left of Figure 4 outlines the behavioural threshold analysis methodology and related steps in broad terms. The right side of Figure 4 expands the 'Construct measurement instrument' step and shows the context of the three themes in this research. The shaded area shows the three main themes and their relevant sub-themes and highlights where this research makes its main contribution and answers the main research question through providing answers to the research sub-questions.

7. Validation

The validation of the aforementioned methodology and resulting measurement instrument by means of an experimental case study is presented in this section. This is followed by a cursory overview of a current real-world application of behavioural threshold analysis for the measurement of group behaviour in information security.

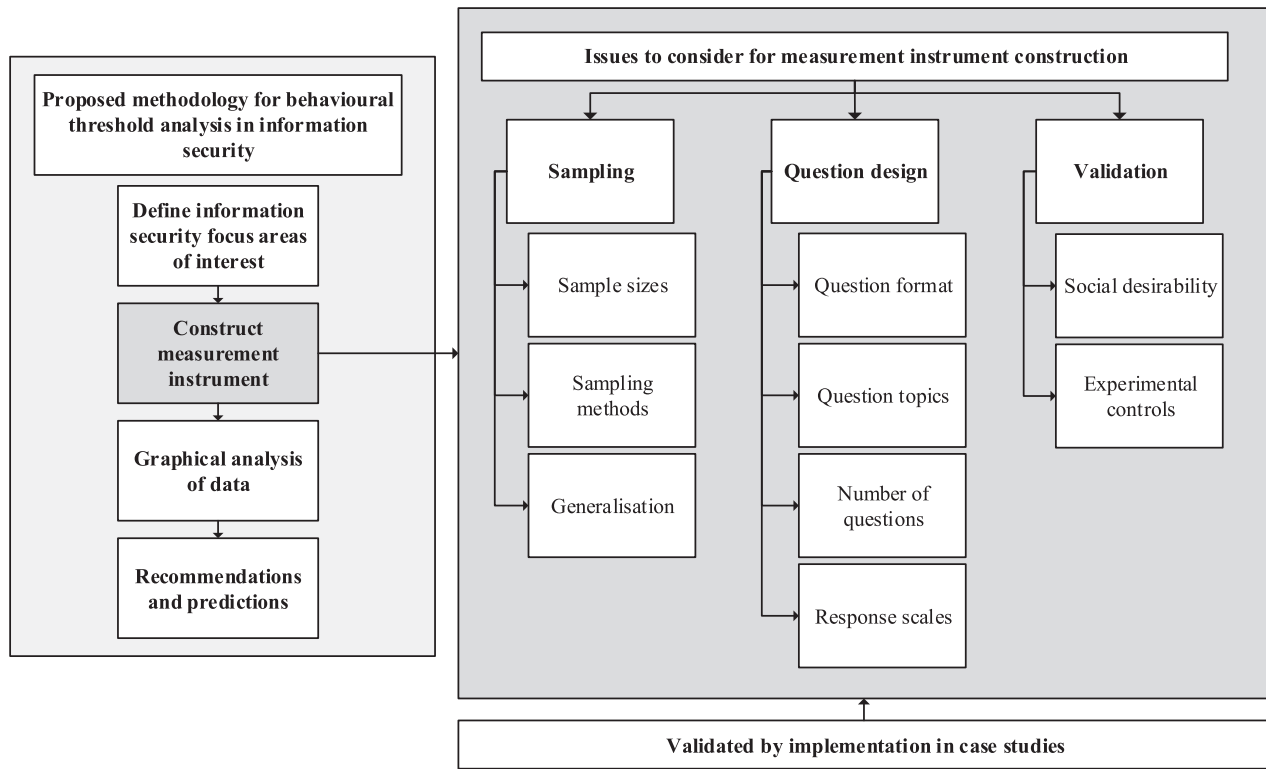


Figure 4. Behavioural threshold analysis for validation case study (Focus area: Internet use).

7.1. Validation case study (Snyman and Kruger 2017b)

In order to further validate the information security questions and questionnaire structure that was determined above, a third case study was conducted with a group of 23 honours-level computer science and information systems students at a university. The following question was presented to the group in the format of Table 2:

‘How inclined would you be to also access torrent websites from devices connected to your university network, given the percentage of students who regularly access torrent websites from devices connected to your university network?’ (Focus area: Internet use).

The question was presented on a projector screen and responses were collected using an optical polling platform (Snyman and Kruger (2017b) present more details on the data collection method). The resulting behavioural threshold graph is presented in Figure 5. The graph indicates the original cumulative thresholds for students’ inclination to also make use of torrent sites (as an example of dubious website use) when a critical percentage of others also uses torrent sites. The eight questions to measure the level of social desirability of participants were included and displayed on the projector screen. The responses for these eight questions were also collected using the optical polling data collection method. Adjustments to the

responses relating to the threshold levels of specific participants, where they showed high levels of social desirability, were made accordingly. See Snyman and Kruger (2017b) for a complete discussion of the results.

It can be seen from Figure 5 that, following the expected trend for threshold analysis, the cumulative thresholds remain above the equilibrium line and only intersect at an 86% participation level. The graph shows an initial incline in the cumulative thresholds,

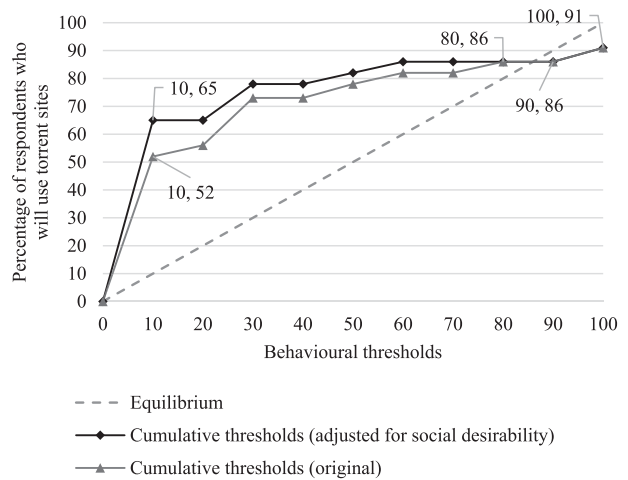


Figure 5. Schematic representation of the methodology of behavioural threshold analysis in information security.

i.e. a willingness to follow group behaviour, with 52% of the group showing a threshold of 10% for participation in using torrent sites. This willingness might be higher than reported due to the level of social desirability that the respondents exhibit. When correcting for the socially desirable answers (see Appendix A), willingness for participation is shown to be higher at 65%. The original cumulative thresholds and the thresholds that were adjusted for social desirability converge before the intersection of the equilibrium line. The group reaches an equilibrium for participation ($m=0$ for both line segments, left and right, of the intersection). This indicates that, in the absence of an extrinsic intervention, 86% of the group will eventually use torrent sites due to the group influence. Ultimately, this analysis indicates that the use of torrent sites is a problem and that the respondents are likely to transgress with this behaviour when they know that enough others in the group are also doing so. Training with regard to torrent sites should therefore typically be included in information security awareness programmes in order to address this behavioural phenomenon.

The results obtained for this validation study further indicate the suitability of the suggested information security questions and the presentation of the questions for behavioural threshold analysis. In comparison to the initial uncharacteristic results in case study 1, case studies 2 and 3 show encouraging results that conform to the expected patterns seen in literature. This was due to the positive effects of the presentation of the questions, i.e. in a grid pattern with threshold intervals. The participants then ranked their inclination towards participating in the behaviour by indicating their response in the grid. The presentation was based (in part) on the suggestions of Pattinson et al. (2016) on combining the methods of questionnaires and the repertory grid technique. The ranking of threshold intervals ensured that the threshold values could effectively be used for the mathematical analysis and prediction of the collective behaviour of the group.

The nature of the questions that were chosen is shown to be suitable for the task, based on the success of the implementation in the validation case study. The social desirability questions were shown to contribute positively to the interpretation of the results by allowing insights into the differences between the reported thresholds when compared to the actual inclinations that the individuals in the group exhibit.

7.2. Real-world implementation

The application of a duly prepared measurement instrument, based on the recommendations provided in this

research, was performed to test the approach in a real-world environment (Snyman, Kruger, and Kearney 2017). Following the guidelines as set out in this paper, a practical experiment was conducted at a large utility corporation in Australia. With the support from management, a department with 63 respondents was identified for inclusion in this study. A complete questionnaire comprising all five focus areas as in Table 1 was used, supplemented with additional questions on positive security behaviour and social desirability. An analysis of the collected responses shows encouraging results and the results relevant to Table 1 are summarised here:

The results showed that the specific department exhibited high behavioural thresholds for *password management*, *internet use*, and *e-mail use*. High thresholds indicate that the respondents are highly aware of the associated risks with following negative examples in the group security behaviour and will therefore not participate in the detrimental actions that are performed by others. In terms of *social media use* and the *reporting of security incidents*, the group showed low behavioural thresholds. This indicates that the group is not sufficiently aware of the risks involved in participating in these behaviours. The respondents are likely to also partake in these behaviours when a critical mass of the group performs these actions. Inclusion of these topics in information security awareness programmes is therefore recommended to ensure that the department is sufficiently trained to avoid questionable information security behaviour.

The success of the practical implementation of threshold analysis in industry is attributed to the detail investigation and testing of the approach as presented here in this paper. Although the research in Snyman, Kruger, and Kearney (2017) only reports on one application, the measurement instrument and methodology are shown to work well in real-world situations. Further applications and expansions of the measurement instrument are planned for future work in other industries and new real-world studies.

8. Reflection

Through the case studies and validations, it was shown that a unique information security behavioural threshold analysis measurement instrument was successfully developed. This instrument addresses the special nature and requirements of threshold analysis and contributes to the enhancement of the methodology of behavioural threshold analysis in the context of information security. The result is also a positive answer to the main research question that was formulated in Section I. The substantiation for a positive answer is presented in terms of the

main themes (relating to the research sub-questions) as described above:

Sampling – The suggested sampling approach is to target a relatively *small* group of respondents in a purposive manner, i.e. they have *specific knowledge* of the behaviour of others in the group. The analysis does *not require any generalisation* of the results to a greater population as the prediction of information security behaviour is limited to the group that is surveyed. In the validation and real-world case studies, the sample sizes were kept small and were determined by a logical delimitation along the lines of organisational structures. The individuals in the group have the required knowledge of the behaviour of others in the group due to their daily exposure to one another. It was possible to obtain useful responses and the prediction of group behaviour, based on the aggregated behavioural thresholds, was successful.

Question design – In terms of question design, it is recommended to identify specific information security topics and present questions relating to the topics in a combination format (a cross between traditional questionnaires and repertory grids). The responses on the grid are limited to a four-point Likert scale to ensure that a respondent either commits to, or rejects the behaviour, given the percentage of others who participate. Due to the number of required responses per question, only one question per information security aspect is suggested. When the suggested question design was implemented, the respondents were guided to supply seemingly correct and useful responses due to the even nature of the Likert scale. By not allowing a neutral response, the scale mimics the binary nature of information security behaviour and it is ensured that each response can be used in the behavioural threshold analysis. The length of the measurement instrument was acceptable and even with the many responses required, due to the grid format, the time that was spent to respond was kept to a minimum. Even though the specific topics were identified to limit socially desirable responses, the group was shown to still have high levels of social desirability, but the effect could be assessed and controlled for.

Validation – Due to the unique nature of the measurement instrument and because it does not conform to the traditional questionnaire format, the usual statistical metrics for measuring reliability and validity cannot be applied in this context. It is therefore up to an expert to evaluate the suitability of the measurement instrument. The sensitivity of themes relating to information security gives rise to social desirability, which in this context, is unfavourable for the eventual behavioural threshold analysis. When the suggested measurement instrument was deployed during the exercises, the effect of the social desirability was measured and controlled adaptations to the responses could be made before the formal analysis. Both the original and adapted behavioural thresholds are then used as part of the analysis to provide a more accurate view on the group's information security behaviour. Finally, the

methodological and practical considerations as presented in this paper can be employed during face validity examination as a guideline for a standard information security behavioural threshold measurement instrument.

In all the case studies, respondents were asked to provide feedback or comments regarding the measurement instrument in terms of how easily they understood the process, how easily they answered the questions and whether they had any suggestions or complaints. Their feedback was in the form of open-ended sentences at the end of each questionnaire. These were supplemented with follow-up discussions and informal interviews on their experiences with the measurement instrument. The feedback they provided was overwhelmingly positive, e.g. 'Love the scaling style of the question', 'The process was easy to follow', 'The questions were clear', etc. This type of feedback further serves to informally support the suitability of the suggested methodology for behavioural threshold analysis in information security in an analogical manner.

9. Conclusion

In this research, the aim was to provide a methodology for the construction of a measurement instrument for behavioural threshold analysis in information security and to provide a solution to the problem statement. Due to the unique requirements of an information security threshold application, traditional information security measurement instruments are insufficient and need considerable adaptation to determine behavioural thresholds.

In providing a methodology for the construction of a measurement instrument for behavioural threshold analysis, the problem of the unique requirements for an application in information security was addressed. This was achieved by determining information security topics and related questions for use in behavioural threshold analysis research in information security. Special attention was also given to the manner in which these questions are presented, both in physical layout and in wording, when used in questionnaires. This article presented the analysis of selected literature relating to information security themes and associated questions to base the specific behavioural threshold analysis questions on a sound theoretical framework. The questions that were identified were implemented in three case studies to test the suitability of the questions when used in experimental circumstances. The manner in which the questions were presented, i.e. in a grid fashion (similar to that of a repertory grid) was also tested in the experimental application of the behavioural

threshold analyses in the context of information security. The results of these experiments indicate the suitability of the identified questions and the manner in which they are presented. Future attention will also be given to the managerial value of information security behavioural threshold analysis and its utility as a management decision support tool to improve the information security of organisations.

Note

1. Based on migratory behaviour of rodents, the lemming effect refers to blindly following a group to one's own detriment.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Dirk Snyman  <http://orcid.org/0000-0001-7360-3214>

References

- Ajzen, I. 1991. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50 (2): 179–211.
- Al-Omari, A., O. El-Gayar, and A. Deokar. 2012. "Information Security Policy Compliance: The Role of Information Security Awareness." In *Proceedings of the 18th Americas Conference on Information Systems (Paper 16)*, 1–10. Seattle, WA: Association for Information Systems.
- Ashenden, D. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13 (4): 195–201.
- Bolarinwa, O. A. 2015. "Principles and Methods of Validity and Reliability Testing of Questionnaires Used in Social and Health Science Researches." *Nigerian Postgraduate Medical Journal* 22 (4): 195–201.
- Butler, R., and M. Butler. 2018. "Some Password Users are More Equal than Others: Towards Customisation of Online Security Initiatives." *South African Journal of Information Management* 20 (1): 1–10.
- Connolly, L., M. Lang, J. Gathegi, and J. D. Tygar. 2016. "The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study." In *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 33–44. Frankfurt, Germany: Plymouth University.
- Crowne, D. P., and D. Marlowe. 1964. *The Approval Motive*. New York: Wiley.
- Cuganesan, S., C. Steele, and A. Hart. 2018. "How Senior Management and Workplace Norms Influence Information Security Attitudes and Self-Efficacy." *Behaviour & Information Technology* 37 (1): 50–65.
- Dahlgren, G. H., and H. Hansen. 2015. "I'd Rather be Nice than Honest: An Experimental Examination of Social Desirability Bias in Tourism Surveys." *Journal of Vacation Marketing* 21 (4): 318–325.
- Da Veiga, A., and N. Martins. 2017. "Defining and Identifying Dominant Information Security Cultures and Subcultures." *Computers & Security* 70: 72–94.
- Dhillon, G., R. Syed, and C. Pedron. 2016. "Interpreting Information Security Culture: An Organizational Transformation Case Study." *Computers & Security* 56 (1): 63–69.
- Dodou, D., and J. C. De Winter. 2014. "Social Desirability is the Same in Offline, Online, and Paper Surveys: A Meta-Analysis." *Computers in Human Behavior* 36: 487–495.
- Fazio, R. H. 1990. "Multiple Processes by Which Attitudes Guide Behavior: The MODE Model as an Integrative Framework." *Advances in Experimental Social Psychology* 23 (1): 75–109.
- Fisher, R. J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning." *Journal of Consumer Research* 20 (2): 303–315.
- Granovetter, M. 1978. "Threshold Models of Collective Behavior." *American Journal of Sociology* 83 (6): 1420–1443.
- Gronney, J. S. 1983. *I Will if You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior*. Bedford, MA: COMAP Inc.
- Helfinstein, S. M., J. A. Mumford, and R. A. Poldrack. 2015. "If all Your Friends Jumped Off a Bridge: The Effect of Others' Actions on Engagement in and Recommendation of Risky Behaviors." *Journal of Experimental Psychology: General* 144 (1): 12–17.
- Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95.
- Kaur, J., and N. Mustafa. 2013. "Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME." In *Proceedings of the 2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286–290. Kuala Lumpur, Malaysia: IEEE.
- Kruger, H. A., and W. D. Kearney. 2006. "A Prototype for Assessing Information Security Awareness." *Computers & Security* 25 (4): 289–296.
- Nguyen, Q. N., and D. J. Kim. 2017. "Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives." In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4947–4956. Hawaii: University of Hawaii at Manoa.
- Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. 2017. "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies." *Computers & Security* 66 (2017): 40–51.
- Parsons, K., A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram. 2014. "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)." *Computers & Security* 42 (2014): 165–176.
- Pattinson, M. R., and G. Anderson. 2007. "How Well are Information Risks Being Communicated to Your Computer End-Users?" *Information Management & Computer Security* 15 (5): 362–371.
- Pattinson, M. R., M. A. Butavicius, K. Parsons, A. McCormac, and C. Jerram. 2015. "Examining Attitudes Toward

- Information Security Behaviour Using Mixed Methods.” In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, 57–70. Lesvos, Greece: Plymouth University.
- Pattinson, M. R., K. Parsons, M. Butavicius, A. McCormac, and D. Calic. 2016. “Assessing Information Security Attitudes: A Comparison of Two Studies.” *Information & Computer Security* 24 (2): 228–240.
- Porter, S. R., M. E. Whitcomb, and W. H. Weitzer. 2004. “Multiple Surveys of Students and Survey Fatigue.” *New Directions for Institutional Research* 2004 (121): 63–73.
- PWC. 2017. *Strengthening digital society against cyber shocks - Key findings from The Global State of Information Security Survey 2018*. Online: Price Waterhouse Coopers <https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf>.
- Ray, J. J. 1984. “The Reliability of Short Social Desirability Scales.” *Journal of Social Psychology* 123 (1): 133–134.
- Redmiles, E. M., Y. Acar, S. Fahl, and M. L. Mazurek. 2017. “A Summary of Survey Methodology Best Practices for Security and Privacy Researchers.” *UM Computer Science Department Technical Reports*.
- Reynolds, W. M. 1982. “Development of Reliable and Valid Short Forms of the Marlowe-Crowne Social Desirability Scale.” *Journal of Clinical Psychology* 38 (1): 119–125.
- Safa, N. S., R. Von Solms, and L. Fitcher. 2016. “Human Aspects of Information Security in Organisations.” *Computer Fraud & Security* 2016 (2): 15–18.
- Scholl, M., K. Leiner, and F. Fuhrmann. 2017. “Blind Spot: Do you Know the Effectiveness of Your Information Security Awareness-Raising Program?” In *Proceedings of the 21st world Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, 361–366. Orlando, Florida, USA: International Institute of Informatics and Systemics.
- Sekaran, U., and R. Bougie. 2010. *Research Methods for Business: A Skill Building Approach*. 5th ed. Chichester, United Kingdom: John Wiley & Sons.
- Shay, R., S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. 2010. “Encountering Stronger Password Requirements: User Attitudes and Behaviors.” In *Proceedings of the Proceedings of the Sixth Symposium on Usable Privacy and Security*, 1–20. Redmond, Washington, USA: ACM.
- Snyman, D. P., and H. A. Kruger. 2016. “Behavioural Thresholds in the Context of Information Security.” In *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 22–32. Frankfurt, Germany: Plymouth University.
- Snyman, D. P., and H. A. Kruger. 2017a. “The Application of Behavioural Thresholds to Analyse Collective Behaviour in Information Security.” *Information & Computer Security* 25 (2): 152–164.
- Snyman, D. P., and H. A. Kruger. 2017b. “Optical Polling for Behavioural Threshold Analysis in Information Security.” In *Proceedings of the International Conference on Information and Knowledge Engineering (IKE'17)*, 39–45. Las Vegas, USA: CSREA Press.
- Snyman, D. P., H. A. Kruger, and W. D. Kearney. 2017. “The Lemming Effect in Information Security.” In *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, 91–103. Adelaide, Australia: Plymouth University.
- Sommestad, T., and J. Hallberg. 2013. “A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance.” In *Proceedings of the IFIP International Information Security Conference*, 257–271. Auckland, New Zealand: Springer.
- Sommestad, T., J. Hallberg, K. Lundholm, and J. Bengtsson. 2014. “Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies.” *Information Management & Computer Security* 22 (1): 42–75.
- Stanton, J. M., K. R. Stam, P. Mastrangelo, and J. Jolton. 2005. “Analysis of End User Security Behaviors.” *Computers & Security* 24 (2): 124–133.
- Tanis, M., and T. Postmes. 2005. “A Social Identity Approach to Trust: Interpersonal Perception, Group Membership and Trusting Behaviour.” *European Journal of Social Psychology* 35 (3): 413–424.
- Vance, A., and M. T. Siponen. 2012. “IS Security Policy Violations: A Rational Choice Perspective.” *Journal of Organizational and End User Computing (JOEUC)* 24 (1): 21–41.
- Van de Mortel, T. F. 2008. “Faking It: Social Desirability Response Bias in Self-Report Research.” *The Australian Journal of Advanced Nursing* 25 (4): 40–48.

Appendix A

Social desirability scales

In case studies 2 and 3, the behavioural thresholds were adjusted to correct for and show the possible effect that social desirability has on the analysis of these thresholds. The table below lists the questions of the social desirability measurement instrument that is commonly used in literature. 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.

Social desirability questions (Ray 1984).

In order to accurately measure the level of social desirability of a respondent, his/her responses to each question are scored on a scale of 1–3, based on their response of Yes, Unsure, or No.

The scores for all the responses are added and provide a possible score between 8 and 24. The higher a respondent’s score on this scale, the higher the probability is that the respondent was not completely honest in answering the preceding questionnaire on information security behaviours.

In this research, only the highest possible score of 24 was taken as the cue to adapt responses to control for the possible effect of social desirability and was done in the following manner: If a respondent with a social desirability of 24 selected his/her inclination of participation for a negative information security behaviour, his/her response was adjusted upwards, e.g. a response indicated as *strongly inclined* (3), was adjusted to *always* (4). This translates to a *lower* behavioural threshold for participation than what the respondent originally reported. For positive behaviour the response is adapted downwards, e.g. from *strongly inclined* (3) to *somewhat inclined* (2). This is due to the high level of social desirability that causes the respondent to overstate his/her willingness to participate in the positive group behaviour. In these cases, the threshold for participation is taken at a *higher* percentage.