Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework

D. P. Snyman, H. A. Kruger

Information security behavioural threshold analysis in practice: An implementation framework

D.P. Snyman[0000-0001-7360-3214] and H.A. Kruger [0000-0001-8514-4422]

School of Computer Science and Information Systems
North-West University, Potchefstroom, South Africa
dirk.snyman;hennie.kruger@nwu.ac.za

Abstract. This paper presents the development of a framework for evaluating group behaviour in information security in practice. Information security behavioural threshold analysis is employed as the theoretical foundation for the proposed framework. The suitability of the proposed framework is evaluated based on two sets of qualitative measures (general frameworks and information security frameworks) which were identified from literature. A novel conceptual mapping of the two sets of evaluation measures is presented and used to evaluate the proposed framework. The successful evaluation of the proposed framework, guided by the identified evaluation measures, is presented in terms of positive practical applications, as well as positive peer review and publication of the underlying theory.

Keywords: Information security group behaviour, framework development, evaluation.

1 Introduction

Many models and frameworks are used throughout information security (InfoSec) literature to determine or explain attitude that individuals exhibit towards InfoSec which is indicative of their eventual behaviour [1]. Such frameworks and models are mainly focussed on the individual's behaviour, and researchers infer that this should apply to group behaviour as well. However, this is not always the case, as there are many other influences on group behaviour, such as the lemming effect, contextual factors, influential people, etc. It is, therefore, not enough to simply expect individual behaviour to be indicative of group behaviour.

To the best of the researchers' knowledge, no framework for analysing and predicting InfoSec group behaviour is currently available in literature. In this paper, a formal framework is proposed for group behaviour in InfoSec. This proposed framework is based in part on aspects found in existing frameworks [1], i.e. norms, beliefs, attitudes, etc. The other integral part of the framework will then consist of those aspects that are specific to group behaviour, i.e. the use of a technique, such as behavioural threshold analysis (BTA) that considers factors, such as the lemming effect and external contextual factors. This paper represents the culmination of an overarching

study in which the use of a BTA approach was conceptualised in terms of group behaviour in InfoSec, and with the abovementioned background in mind, the aim of this study is now firstly, to *formalise a framework for evaluating information security group behaviour in practice, supported by behavioural threshold analysis as the underlying theory* thereby allowing InfoSec practitioners to utilise the approach, and secondly, to *critically evaluate the proposed framework based on qualitative measures from literature*.

The remainder of this paper is structured as follows: In **Section 2,** a brief contextualisation for applying research in practice and a theoretical view on the requirements of a successful framework are presented. In **Sections 3** and **4** the development of the resulting framework and the evaluation thereof, based on the requirements from Section 2 are described. A discussion on the general and specific contributions of the resulting framework is presented in **Section 5** and the paper is concluded in **Section 6**.

2 Literature review

2.1 Contextualisation

Translating research findings and recommendations of any nature into practice remains an elusive process [2-4]. Some of the reasons why this general disconnect exists between most types of research and the related acceptance thereof in practice include ambiguity in existing research [3, 5]; limited published reflection on implementation [5]; ongoing research is often still inconclusive [4]; decision makers lack the required information [6]; and attitudes and beliefs of individuals [3, 7] which translates to social and cultural resistance to the change associated with implementation.

This disconnect between research and practice has also been identified in the domain of InfoSec [5, 8], where it especially holds true for non-technical aspects of InfoSec such as InfoSec awareness and behaviour. Research into human behaviour (and how it relates to InfoSec behaviour and culture) is often based on, and guided by, theoretical models from the fields of sociology and social psychology. While such models can assist in uncovering the intricacies of behaviour by highlighting complexity and structuring the underlying themes, they do not necessarily provide for simple integration into actionable methods in practice.

The level of success of such an integration is, however, subject to three criteria, namely *Evidence*, *Context*, and *Facilitation* [4] (ECF). In terms of research pertaining to InfoSec (specifically security culture), AlHogail [8] suggests following the STOPE approach [7] to facilitate change when implementing new approaches to effect change in the culture and the eventual underlying behaviour. The dimensions to be adhered to for STOPE are *Strategy*, *Technology*, *Organisation*, *People*, and *Environment*.

These criteria and dimensions are therefore subsequently used to guide and evaluate the development of a framework for applying the BTA approach, in the context of InfoSec, in practice.

2.2 Framework requirements

The qualitative criteria for evaluating frameworks in general (*Evidence*, *Context*, and *Facilitation*) and for frameworks for InfoSec (STOPE) will be presented here in detail and contextualised in terms of research in general versus InfoSec research. Finally, a mapping of how these two approaches align, and how they relate to this research is presented.

Evidence, Context, and Facilitation

In terms of an implementation framework, the interaction between Evidence (E), Context (C), and Facilitation (F) is said to determine the eventual Successful Implementation (SI) of the framework in practice, i.e. SI is a function of three criteria [4] so that

$$SI = f(E, C, F) \tag{1}$$

The success of the implementation is therefore dependent on the level of maturity by which each of the criteria is met. Each of the criteria and what each represents in terms of a framework is briefly described here. Where applicable, these criteria are already presented in terms of InfoSec:

Evidence – Evidence refers to the level of scrutiny that the model or approach that underpins a framework has undergone. Is there substantiated proof that the model is fit for purpose? [4]

Context – Context is concerned with the setting in which a framework is to be applied in practice. In general, this refers to the physical attributes of the environment such as buildings, people, and processes [9]. However, for the successful implementation of a framework, this view might be too narrow, since in essence context also implicitly refers to intangible qualities, such as individual and group behaviour, and the underlying (security) culture [3, 9].

Facilitation – Implementing research in practice is essentially a process whereby change of some kind is sought to be effected. Change is a process that ought to be facilitated if it is to be successful and long-lived [3]. Such facilitation refers to the understanding of (and ultimately altering) attitudes and behaviours, specifically by leveraging the way in which "an individual is able to influence other individuals' attitudes or overt behaviour" [3, 10]. In terms of InfoSec, Snyman and Kruger [11] hypothesise that while some people may inherently be more influential [3], the behaviour of all individuals exerts influence on the eventual behaviour of a group.

STOPE

InfoSec frameworks may be evaluated by means of a critical evaluation of how well the framework addresses *Strategy*, *Technology*, *Organisation*, *People*, and the *Environment*. Each of these dimensions is briefly explained below, based on the work of AlHogail [8] which contextualises them in terms of InfoSec.

Strategy – Strategy refers to the suggested measures that are applied to effect change within an organisation to improve its overall levels of InfoSec. These ap-

proaches may include the implementation of formal plans of action, such as InfoSec policies and guidelines as well as the structured approach of a framework.

Technology – In this context, technological means of addressing InfoSec is referred to as technology. Frameworks should ideally provide for changes or improvements on the technical measures that are used to safeguard systems.

Organisation – The success of strategy is reliant on the underlying security culture of an organisation. This culture and eventual behaviour are often influenced by the way in which an organisation is structured. A framework should provide guidelines for how structures within an organisation will influence the application thereof and, ideally, how structures may be leveraged to achieve the goal of the framework.

People – InfoSec ultimately revolves around people. It is often people that undo security due to unwanted actions. Frameworks should seek to address the human aspect of InfoSec in terms of behaviour, culture and awareness.

Environment – Environment view refers to the greater context in which an organisation has to address InfoSec, and which should be included in the application of a framework. On a macro level, this may include concepts, such as regulatory frameworks and legislation [8], but on a smaller level can refer to the context in which an individual or group behave in terms of InfoSec [9].

Mapping STOPE to ECF

An assessment of the framework evaluation criteria as mentioned in Sections 2.1 and 2.2 above allows for a combination of the two approaches by means of a conceptual mapping. Table 1 shows the conceptual mapping of STOPE to ECF:

Table 1. Conceptual mapping of STOPE to ECF

Evidence	*Context*	*Facilitation*
Peer review combined with resulting STOPE evaluation	O:Organisation P:People E:Environment	S:Strategy T:Technology

From Table 1, it can be seen that the individual views from STOPE could not as easily be mapped to Evidence (ECF), as all these views can contribute in some way to this criterion. It is concerned with the rigour of the underlying model on which a framework is based. It stands to reason then, that in combination with other types of measures that can confirm said rigour (e.g. peer review, or experimentation), evidence can thus be conceptualised as the resulting evaluation that is conveyed by STOPE. However, in the context of this research, Evidence will be used as a freestanding criterion, evaluated on the available peer review, case studies, and successful implementations. For the remaining criteria, the Organisation, People and Environment from STOPE [8] can be directly mapped to Context [3] from ECF. Overlapping themes include people, behaviour, culture, and physical attributes of the environment. In the final instance, Facilitation (ECF) encompasses the strategy and technology views from STOPE. The common concepts from these constructs that can be identified are the approaches for achieving positive change through organisational, technological, and human means.

3 Framework model and development

In order to describe the development of the suggested framework, the underlying theoretical model should first be presented. In this section, the aim is to firstly summarise the BTA model as implemented in the greater research project, followed by a description of the resulting framework and its elements.

3.1 Behavioural threshold analysis model

Group behaviour is a complex phenomenon. To analyse this complexity, Granovetter [12] describes a theory called "Threshold models of collective behaviour". The model described by Granovetter is used as the underlying theoretical grounding for the framework. In short, the model takes into account the mechanisms whereby individuals influence the behaviour of each other, i.e. based on an intrinsic inclination of an individual to follow the example of existing group behaviour. This inclination to follow behaviour is conceptualised as the individual's behavioural threshold. The said threshold is expressed as a percentage of group members who perform a behaviour that will sway an individual to participate in the specific behaviour. When the (perceived) participation rate of group members exceeds the behavioural threshold of the individual, the individual will follow the group's example and also perform the behaviour. When participation in group behaviour exceeds an individual's threshold for participation, the individual might even perform group behaviour that is contrary to his/her convictions and predisposition.

Growney [13] describes how the model can be implemented in circumstances where groups of individuals congregate and how the mathematical aggregate of behavioural thresholds may be interpreted to allow for a prediction of eventual group behaviour. The model was successfully applied in InfoSec in earlier, related studies and the reader is referred to these sources for in-depth reading on the application of BTA in InfoSec [11, 14, 15].

3.2 Development of information security group behaviour framework

In Section 1, reference was made to the first aim of this research, namely, to formalise a framework for the practical application of BTA in InfoSec. To address this aim, Figure 1 shows the proposed framework for evaluating group behaviour in InfoSec and illustrates the overarching development and categorises different epochs of the framework's development. Each of the epochs is subsequently briefly described below.

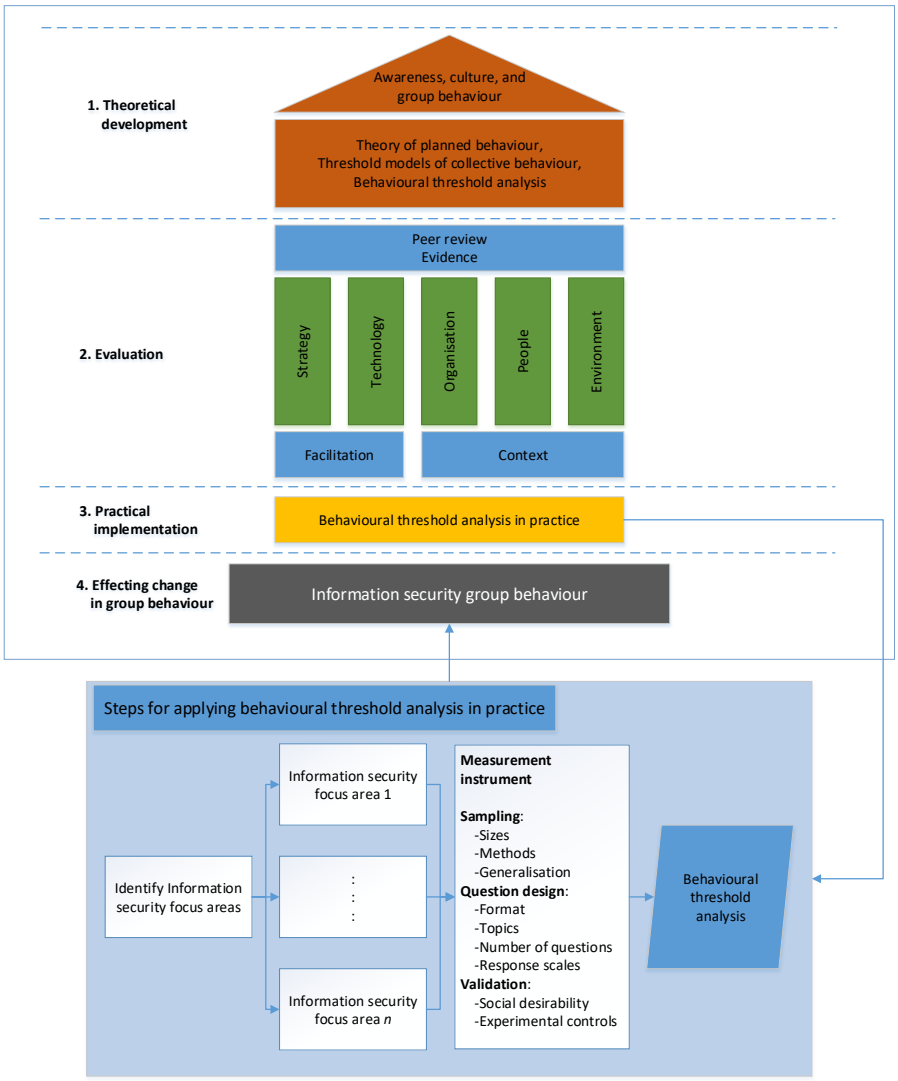

Fig. 1. Framework for the evaluation of information security group behaviour in practice

1) Theoretical development – This epoch refers to the investigation into group behaviour in InfoSec. It includes a review of the related literature on the following themes: human behaviour in general and in the context of InfoSec; modelling human behaviour, e.g. the theory of planned behaviour, and its employment in security awareness and security culture; and group behaviour (threshold models of collective behaviour) and the analysis thereof (BTA). The development of the underlying theory also comprises the development of methodological and practical guidelines for experimental and practical applications.

2) Evaluation – Based on the aforementioned ECF criteria and STOPE views, the evaluation epoch refers to a formal evaluation of the underlying theoretical assumptions and the framework itself. In the following section (see Section 4), a formal evaluation of the proposed framework is shown.

3) Practical implementation – After a successful evaluation, evidencing a well-founded theoretical basis and framework, the approach is ready for implementation. The blown-up view shows the minutia of the application of BTA in InfoSec.

4) Effecting change in group behaviour – The results of the BTA application may be interpreted to detect areas of InfoSec that need intervention to improve behaviour.

In the following segment (Section 4), how the combination of ECF and STOPE was employed to evaluate the proposed framework is shown.

4 Framework evaluation

During the related research and the development of BTA as an approach for InfoSec, the requirements for ECF and STOPE were met. In this section, the extent to which peer review and practical applications contribute to the maturity of the framework is described.

4.1 Peer review and publication

Table 2 shows the STOPE criteria and ECF views. A critical evaluation and motivation are provided.

Table 2. Critical evaluation of the proposed framework

	STOPE criteria	**Critical evaluation and motivation**	*Evidence* (peer-reviewed publications)
Context	Organisation	One of the main c*ontexts* with which BTA is concerned, is that of the *Organisation*. The ultimate outcome of the successful implementation of the approach is improved levels of InfoSec within any organisation where it is applied. A collection of papers, both in InfoSec journals and conference proceedings, were published that contribute to the rigour of the underlying theoretical model and approaches.	Organisation forms part of all of the previous papers [9, 11, 14-18] which cannot be listed here due to space constraints. Refer to the References section for full bibliographical details.
	People	BTA is based on the behaviour and interaction of people. All the previous work [9, 11, 14-18] therefore encompasses the *People* view; however one paper is highlighted here: Developing the interrelated concepts of sequential decision-making and information cascades in InfoSec, a novel view of the *context* of how InfoSec behaviour is formed was peer-reviewed, published and presented at an international conference.	*Theorising on information cascades and sequential decision making for analysing security behaviour* [17]
	Environment	Given the influence of the *environment*, and its many facets on behaviour, a paper on the *contextual* factors that influence InfoSec behaviour was presented at an international conference after peer review and published in the proceedings.	*External contextual factors in information security behaviour* [9]

Facilitation	Strategy	A paper that describes and validates the underlying methodology, including some practical considerations for BTA in InfoSec, was published in a peer-reviewed journal. This contributes to formalising the *strategy* to *facilitate* positive change in InfoSec.	*Behavioural threshold analysis: Methodological and practical considerations for applications in information security* [14]
	Technology	With the aim of facilitating and partially automating BTA, a novel data collection method (optical polling) and decision support system (DSS) were developed. This *technology* can help *facilitate* the practical aspects of the model implementation. The novel data collection and the DSS was presented at an international conference and published as a peer-reviewed book chapter.	*Optical polling for behavioural threshold analysis in information security* [16]; *A management decision support system for evaluating information security behaviour* [18]

The applications of the approach in practice are presented in the following subsection.

4.2 Applications in practice

Throughout the development of the approach to apply BTA in InfoSec, practical experiments were conducted to test the working of the model within this context. An initial pilot study was conducted to test the feasibility of the model [11]. After further development of the approach and the underlying theoretical foundations, such as the required methodological approach [14], two successful practical applications were conducted.

The first practical application of BTA was conducted at an Australian utility company [15]. The resulting insights and recommendations regarding employees' InfoSec behaviour were communicated in a report to the company. Feedback indicated that the insights were found to be invaluable in guiding the directions of future awareness campaigns.

The second application was in an academic context at a South African University [9]. The results from the exercise correlated with the expected and observed InfoSec behaviour of students in a university residence. The success of these practical applications, the commonalities and differences between the different contexts where the approach was applied, and the reporting publications passing peer review, verifies that this procedure for application (as presented in this framework) is effective.

5 Contributions

A twofold discussion of the successes of the framework is presented here in terms of general and specific contributions to the field of InfoSec.

5.1 General

This research contributes to the general field of InfoSec by having 1) contributed a methodology for formalising a framework for the analysis of group behaviour in In-

foSec; 2) synthesised qualitative measures to critically assess and evaluate frameworks in InfoSec by conceptually mapping methods from literature; and 3) contributed an approach to measure InfoSec group behaviour to improve the management thereof and influence change in behaviour. Supplementary to the general contributions above, certain specific contributions were made and are highlighted next.

5.2 Specific

Reflecting on the specific contributions of this research in terms of the initial research aims relating to the proposed framework, the following is pertinent: 1) BTA is identified as a mechanism to evaluate InfoSec group behaviour and expressed as a well-founded underlying theory for this framework; 2) The framework was critically evaluated in terms of the qualitative measures conceptualised from literature, and furthermore, the approach outlined in this framework was successfully applied in practice which further illustrated the suitability of the framework; 3) The framework can be construed as an instrument for appraising InfoSec awareness in organisations which allows InfoSec practitioners to effect positive change in InfoSec behaviour; 4) A methodology for identifying InfoSec focus areas was identified; and 5) An instrument was contributed that is novel in comparison to existing tools for analysing InfoSec group behaviour with respect to its sensitivity towards the influence of external stimuli, such as contextual factors and the lemming effect.

6 Conclusion

In this paper, a formal framework for the evaluation of group behaviour in InfoSec was presented. The framework is based on BTA as the central theoretical model. Two qualitative evaluation methods for frameworks were identified from literature and contextualised in terms of InfoSec group behaviour. A combination of the two evaluation methods was used to evaluate the fittingness of the proposed framework for analysing InfoSec group behaviour. Based on the resulting evaluation, grounded in scientific peer review, as well as successful applications in practice, the proposed framework was deemed to be fit for purpose.

References

1. Pham, H., Brennan, L., Richardson, J.: Review of behavioural theories in security compliance and research challenge. In: Informing Science and Information Technology Education Conference, Vietnam, pp. 65-76. Informing Science Institute (2017)
2. Grimshaw, J.M., Eccles, M.P., Lavis, J.N., Hill, S.J., Squires, J.E.: Knowledge translation of research findings. Implementation science 7, 50 (2012)
3. Kent, B.: Implementing research findings into practice: frameworks and guidance. International Journal of Evidence-Based Healthcare 17, S18-S21 (2019)
4. Kitson, A., Harvey, G., McCormack, B.: Enabling the implementation of evidence based practice: a conceptual framework. BMJ Quality & Safety 7, 149-158 (1998)
5. Tsohou, A., Kokolakis, S., Karyda, M., Kiountouzis, E.: Investigating information security awareness: research and practice gaps. Information Security Journal: A Global Perspective 17, 207-227 (2008)
6. Haines, A., Donald, A.: Making better use of research findings. British Medical Journal 317, 72-75 (1998)
7. Bakry, S.H.: Development of security policies for private networks. International Journal of Network Management 13, 203-210 (2003)
8. AlHogail, A.: Design and validation of information security culture framework. Computers in Human Behavior 49, 567-575 (2015)
9. Snyman, D.P., Kruger, H.A.: External contextual factors in information security behaviour. In: 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), pp. 185-194. SCITEPRESS – Science and Technology Publications, Lda. (2020)
10. Rogers, E.M.: Diffusion of innovations. Simon and Schuster, New York, NY (2010)
11. Snyman, D.P., Kruger, H.A.: The application of behavioural thresholds to analyse collective behaviour in information security. Information & Computer Security 25, 152-164 (2017)
12. Granovetter, M.: Threshold models of collective behavior. American Journal of Sociology 83, 1420-1443 (1978)
13. Growney, J.S.: I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior. COMAP Inc., Bedford, MA (1983)
14. Snyman, D.P., Kruger, H.A.: Behavioural threshold analysis: Methodological and practical considerations for applications in information security. Behaviour & Information Technology 38, 1-19 (2019)
15. Snyman, D.P., Kruger, H.A., Kearney, W.D.: I shall, we shall, and all others will: Paradoxical information security behaviour. Information & Computer Security 26, 290-305 (2018)
16. Snyman, D.P., Kruger, H.A.: Optical polling for behavioural threshold analysis in information security. In: International Conference on Information and Knowledge Engineering (IKE'17), pp. 39-45. CSREA Press (2017)
17. Snyman, D.P., Kruger, H.A.: Theorising on information cascades and sequential decision-making for analysing security behaviour. 5th International Conference on Information Systems Security and Privacy (ICISSP2019), pp. 205-212. SCITEPRESS – Science and Technology Publications, Lda., Prague, Czech Republic (2019)
18. Snyman, D.P., Kruger, H.A.: A management decision support system for evaluating information security behaviour. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (eds.) Information and Cyber Security - 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings, pp. 1-13. Springer International Publishing (2020)