Deliver Security Awareness Training, then Repeat: {Deliver; Measure Efficacy}

Tapiwa Gundu
Stephen Flowerday
Karen Renaud

This is the accepted version of a paper presented at 2019 Conference on Information Communications Technology and Society (ICTAS), Durban, 6-7 March 2019, which will be published by IEEE.

The final version of the paper is available at: [add link/DOI]

2019 Conference on Information Communications Technology and Society (ICTAS)

Deliver Security Awareness Training, then Repeat: {Deliver; Measure Efficacy}

Tapiwa Gundu
Sol Plaatje University
Chapel St & Bultfontein Rd
Civic Centre, 8301
Kimberley, South Africa
Email: tapgun@gmail.com

Stephen Flowerday
Rhodes University
Drosty Rd
Grahamstown, 6139
South Africa
Email: s.flowerday@ru.ac.za

Karen Renaud
Abertay University
Bell Street
Dundee, DD1 1HG, Scotland
University of South Africa
Email: k.renaud@abertay.ac.uk

***Abstract*—** Organisational information security policy contents are disseminated by awareness and training drives. Its success is usually judged based on immediate post-training self-reports which are usually subject to social desirability bias. Such self-reports are generally positive, but they cannot act as a proxy for actual subsequent behaviours.

This study aims to formulate and test a more comprehensive way of measuring the efficacy of these awareness and training drives, called ASTUTE. We commenced by delivering security training. We then assessed security awareness (post-training), and followed up by measuring actual behaviours. When we measured actual behaviours after a single delivery of security awareness training, the conversion from intention to behaviour was half of the desired 100%. We then proceeded to deliver the training again, another two times.

The repeated training significantly reduced the gap between self-reported intention and actual secure behaviours.

Keywords: information security awareness, information security assessment, intention behaviour gap

I. Introduction

Most of the primary information security focus has been on deploying technical countermeasures to repel attackers [1]. Yet there is an increasing awareness of the reality that, despite all these measures, an organisation's success or failure ultimately depends on the actions of its employees [2], [3]. Insiders, unlike malicious outsiders, have legitimate and widespread access, and can thus wreak havoc simply by making a mistake or unthinkingly carrying out an insecure action.

Regular interventions are carried out to urge maximum employee awareness of secure practice [4]–[6]. It is hoped that these awareness drives will encourage the emergence of a security-aware culture so that good practice will subsequently become the norm. The effectiveness of security awareness drives is, unfortunately, hard to gauge. Most organisations administer post-training tests to provide a measure of the success of the training. Such tests actually only gauge: (1) initial receptiveness, (2) short-term retention of security knowledge, and (3) an employee's self-reported intention to behave securely in the future. If these measures are positive, the organisation subsequently labours under a false sense of reassurance that employees, being aware of good practice, will behave securely.

However it has been shown that, regardless of their assessed knowledge and stated intentions, some employees will not fully comply with their organisation's security policies [7], [8].

It would be helpful if an organisation had a way to come up with a single quantification for their security awareness drives. This quantification measure should encapsulate measures of intention, knowledge and awareness. However, the logistics of these delivery programmes is also important [2], [9]. How many people received the training, for example, and how frequently they received training plays a role [10]. There is also a need to determine whether people convert their intentions to actual behaviours [11], which is by no means a given.

Gauging the effectiveness of training is undeniably challenging, which is why most use post-intervention questionnaires as a proxy. A decade ago, there was no agreed mechanism for gauging the effectiveness of awareness drives [12], [13], but over the last few years a number of measurements have emerged that can be used as indicators of effectiveness. For instance, a scale for measuring behavioural intention has been proposed [14], a questionnaire measures security knowledge [15], and one measures security awareness [16]. Each of these measures one specific aspect of awareness and training effectiveness in a rigorous way.

The challenge of InfoSec's Behavioural Assessment and Awareness Criteria is not only recognized by academia, but also by industry. To balance and enrich this discussion, a number of industry-specific white papers were included in our review.

Many organisations deliver training once, and then check the box, considering that the necessary information has been imparted. Very few employees, according to a recent survey, receive regular or repeated security awareness training [16].

The main objective of the research presented in this paper is therefore to propose a mechanism for quantifying the effectiveness of safety awareness training programmes. This will include a component that measures attitude, knowledge and intention, but also a component to reflect actual behaviours as well as a component that is related to actual delivery of security awareness training [17]. We developed an

ISBN 978-1-5386-7365-2/19/$31.00 ©2019 IEEE

assessment mechanism that can be used to assess the efficacy of security awareness drives. We call the mechanism ASTuTE (Assess SecuriTy Training Effectiveness) and it is based on the *Theory of Planned Behaviour* and the *Knowledge, Attitude and Behaviour Theory*. This, we believe, will help organisations to establish more effective security awareness drives.

II. RELATED RESEARCH AND TRENDS

The majority of those who deliver InfoSec training assess the quality of the training by using a post-assessment quiz. This arguably measures how well the knowledge was communicated and understood. It is also common for people to be asked about their intention to behave securely straight after the training session. This approach hopes that behavioural intentions are a reliable proxy for actual behaviours, and assumes that knowledge is all that is required.

Failure to measure the effectiveness of training may expose organisations to the following preventable errors:

1) Pursue an ineffective awareness / training programme without any real improvement in behaviour.

2) Interrupt an effective awareness / training intervention based on an erroneous subjective assessment, mainly because of a wrong perception that it is not changing behaviour or as being too costly in terms of employee time.

3) It may also be that the organisation believes that everyone is behaving securely anyway, so that no further training is needed.

InfoSec has a limited budget, therefore, there is always the need to justify spending for implementing of controls [18]. Hence, for InfoSec resources to be retained or increased, their expected benefits should be quantifiable.

However, a number of recent studies conclude that intentions are not infallible predictors of behaviours. In terms of secure behaviour assessment, only actual behaviours after awareness and training can reliably be measured, otherwise we are not measuring the actual impact of security awareness training, only stated intentions and short-term retention of facts.

The research literature in various fields confirms the gap between awareness / knowledge and behaviour. For example, hand washing [19]–[21], ethics [22], smoking [23], [24], and environmentally-friendly behaviour [18], [25]. It is therefore questionable whether any intervention aimed only at imparting knowledge, improving attitude and engendering good intentions will be as efficacious as anticipated.

A standard way of carrying out security awareness drive efficacy assessment has not yet emerged. What to measure and how to measure are two distinctive challenges for developing a measurement tool [12]. In an attempt to counter these problems Kruger and Kearny [12] identified three dimensions, knowledge (what an employee knows), attitude (what an employee thinks) and behaviour (what an employee does). On the other hand, Safa et al. [26] suggests dimensions such as involvement, attachment, commitment and the personal norms, while Posey et al. [27] argue that fear of sanctions, incentives, motivation and pride should be measured.

Davis [28] likewise, believes that assessment of InfoSec behaviour is intricate, However endeavors to assess it by measuring knowledge and behavioural intent. However, InfoSec audit results, lost productivity, user satisfaction and knowledge are suggested by Chapple [29]. The European Network and Information Security Agency [30] recommends the measuring of process improvement, attack resistance, efficiency/effectiveness and internal protections. Literature exposes the lack of agreement regarding what to measure and how its measured.

III. THEORETICAL BACKROUND

The Theory of Planned Behaviour (TPB) postulates that behavioural intentions are the motivator employee behaviour [31]–[36]. Behavioural intentions are a function of the employee's behavioural attitude, subjective standards of behavioural performance, and the employee's perception of the ease with which the behaviour can be performed (behavioural control) [31]. TPB suggests that stronger behavioural intentions are more likely to convert to actual behaviour.

Kruger and Kearney [12] proposed the theory of *Knowledge Attitude & Behaviour* (KAB). Its main purpose being the facilitation of factors that lead to secure behaviour. KAB is regarded as an influential explanatory theory for predicting employee intention to behave in a secure manner [16], [37]. Awareness and training at InfoSec provide employees with knowledge and help to generate attitudes that, in combination, help employees formulate their behavioural intentions. [12]. However, what is missing in these two theories is a practical relationship between actual behaviour and behavioural intentions.

ASTUTE extends Kruger and Kearney's [12] "Knowledge, Attitude & Behaviour" model to measure post-training awareness. We then add two additional components: (1) Training Delivery Logistics, and (2) Actual Secure Behaviour Assessment.

IV. THE ASTUTE METHOD

At the time of writing, the assessment of effectiveness and impact of training on InfoSec has no commonly accepted standard [12]. Being used currently are a number of different qualitative and quantitative awareness measures. This research therefore attempts design, conceptualize and validates a novel mechanism for InfoSec training assessment, as shown in Figure 1.

The measurements of the ASTUTE components deliver a holistic insight into the effectiveness of security awareness and training programmes:

Construct one (C1) is concerned with the delivery aspects of InfoSec assessment. These aspects include number of employees trained, how often the employees are trained and the scores of the employees (pass rates).

Construct two (C2) addresses awareness assessment as

suggested by the Kruger and Kearney's [12] knowledge, behaviour and attitude constructs.

Construct three (C3) covers the behavioural assessments. These are focused on aspects like statistics from antivirus software, recorded incident logs and observations that are made.

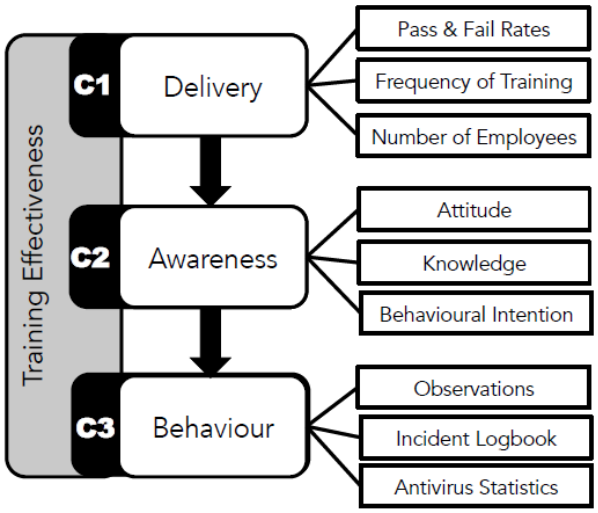

Figure 1: ASTUTE Training Assessment mechanism

1) *Delivery Assessment*: It is beneficial for an organisation to include operational measures to their InfoSec assessment. E-learning is one of the most efficient tools for delivery reporting. Most organisations are making use of e-learning awareness programmes. These learning management systems used to administer knowledge provide a variety of reports. These includes dimensions like number of employees trained, and post-training assessment scores.

2) *Awareness Assessment*: Once routine awareness reports have been established on a regular and accurate basis, more in-depth assessments, such as the evaluation of intent, become necessary. Whether or not InfoSec is directly related to InfoSec's behaviours is determined by these measures. Meaning they determine whether training has the desired effect with regards to employee security behaviour and organisational security culture.

When determining the intent attributes to be captured, it is important to consider the key determinants of security behaviour from the employee's point of view. It can be argued that the organisation's overall security position is better of when its InfoSec objectives and requirements and the attitudes, knowledge and behaviours of its employees are aligned [38].

3) *Behaviour Assessment:* Prior to assessing intention, problematic behaviour (also called target behaviour) and desired behaviour (also called replacement behaviour) must be clearly defined. In other words, they must be accurately stated in observable and measurable terms.

This assessment mechanism proposed by ASTUTE aims to guide professional judgment regarding the safe behaviour of employees. It can be used to evaluate awareness and effectiveness training initiatives by measuring results.

V. RESEARCH METHODOLOGY

Development of the mechanism was done through the application of a qualitative approach. For an understanding of the manifestation of behaviours in the InfoSec context, Literature review of effective behavioural change factors was done within InfoSec, behavioural studies and psychology realm. This led to the designing and development of the initial mechanism. Improvements made by four cycles of research helped to refine and improve the mechanism. The research was conducted at a civil engineering firm in South Africa, where thirty of its employees voluntarily participated in the study.

A. Data Collection

The collection of primary data was facilitated by the use of web-based questionnaire / survey tests, observations, and the incident logbook. Actual behaviours were collected using the behaviour aspect of ASTUTE, behavioural intention was collected the awareness aspect and the operational controls were assessed by the delivery aspect. Secondary data was collected from published articles and books.

B. Data Analysis

The comparison between the awareness and behaviour aspect revealed the gap from intents to actual behaviours. Behavioural patterns were identified using the coding and categorization processes described by Littman [39]. In this study, the data collected was weighted similarly to Kruger and Kearney's [12] method. The importance scaling was however influenced by literature, and management of organisation. The weighting was as follows: Delivery 15%, Awareness 35% and Actual Behaviour 50%.

The data analysis was performed after each iteration and compared with the results of the subsequent iteration to evaluate changes in the InfoSec behaviours of the employees. The total duration of the research was 11 months and consisted of three cycles with about 3.5 months between them. The three iterations had similar activities:

1. Delivering security awareness and training
2. Measuring awareness

VI. FINDINGS AND DISCUSSION

The results of the online questionnaire provided context as well as an overview of the organisation's employees InfoSec knowledge levels. Observations of the employees assisted with first hand experience of how they behave in real life situations. Lastly, document surveys (incident log book and Antivirus/firewall report) highlighted the rate of occurrence of security breaches during the reporting period.

Awareness Assessment: The survey questions collected information based on the intention attributes. Knowledge, attitude and behavioural intention was assessed by these questions.

Behaviour Assessment: this assessment was conducted with the aid of statistics from the antivirus, firewall, incident reports and general observations. Employee security behaviours or intentions to comply, as well as their training

needs were highlighted by these assessments.

During the first iteration, an inadequate understanding of identity theft, importance of firewall, malware, encryption and phishing was revealed These inadequacies became topics for subsequent awareness / training session. These results helped to motivate for resource allocation for subsequent InfoSec awareness and training.

The processing of the findings and importance weightings was done in a spreadsheet application. Presentation of the output was in tabular form, graphical and as awareness maps, as Kruger and Kearney [12] did in their study. The data presented reflected evidence from the intervention to support the propositions relating to security behaviours. The findings of the empirical study are summarized in Table 1

Table 1: Summary of findings

#	Delivery	Awareness	Behaviour	%
1	N/A	18	N/A	18/35 (51%)
2	N/A	28	N/A	28/35 (80%)
3	13	32	32	(13+32+32)/100 (77%)
4	13	33	44	(13+33+44)/100 90%

Iteration 1 comprised two activities. Implementation of awareness campaigns and training was the first activity. This is regarded as important because despite having InfoSec policies in place, employees might not comply to them because of lack of awareness of their existence or understanding of their contents [40]. Literature generally agrees that awareness and training increases employee knowledge. The InfoSec position of management (subjective norms) are conveyed to the employees through this channel, this is in line with our baseline theories. Theories also associate knowledge with alterations of beliefs and attitudes. After the campaign, it was necessary to re-evaluate the effectiveness of the training in order to compare the results with the initial assessment. The evaluation during this iteration was carried out using Kruger's [12] assessment tool, which measures employees' attitudes, knowledge and behavioural intent towards information security, as well as their perceptions of and concerns about the approaches to safeguarding the information asset in the workplace. This tool does not assess actual security behaviour and delivery aspects. This is why it is not applicable (N/A) in Table 1. However, it follows that the behavioural intentions will be equal to the actual behaviours. As shown in Table 1, the average behavioural intention score of the employees was 51% (score of 18 out of 35 questions correct). This revealed a lack of awareness and knowledge.

Iteration 2 was carried out because the security behaviour levels after iteration 1 had increased but not to the levels deemed to be acceptable by the researchers and the organisation's management. Table 1 shows a 51% to 80% (average of 30 out of 35 questions correct) increase that after the first awareness and training initiative. This gave a reflection of positive change in knowledge and intention which was however, in contrary to the actual behavioural change. This highlights the flaws in the belief that behavioural intentions reliably lead to actual behaviours.

Iteration 3 was similar to iteration 1 and 2. However, the difference from the prior assessments was that it was carried out using ASTUTE. This made it possible to compare results actual behaviour vs behavioural intentions. During this iteration, behavioural intentions scored 91% and this gave a comforting sense of security. However, the actual behaviour measurement was 55%. This iteration gave a more accurate sense of effectiveness. During this iteration, the proposed assessment tool was used. The behavioural intent measure changed from 80% in the second iteration to 91% (average of 33 out of 35 questions correct) in the third. This assessment was not only based on intention, but also on awareness and behavioural measures. These additional measures reduced the overall security assessment picture to 77%, after 80% in the previous iteration.

Iteration 4 comprised two activities. This iteration was necessitated by the emergence of a gap between intention and actual behaviour during Iteration 3. The purpose was to attempt to reduce the gap by training repetition, to ensure that intention and awareness was converted to actual behaviour. Repetition, is known to influence conversion of intentions to actual behaviour. Which then leads to formation of habits. Habits are ultimately incorporated into employee culture. Behaviours that are not habitual require cognisant thinking to carry them out, thus less likely to be carried out due to the substantial effort required.

In the fourth iteration, ASTUTE was used again. The delivery measurement did not change from the previous iteration, as there was no change in the number of trained staff nor in the training frequency. Thus, the success rate remained stable. During this iteration, the behaviour improved from 77% to 90%.

VII. LIMITATIONS AND RECOMMENDATIONS

The data was collected from one South African organisation. A larger sample size could improve the generalizations of the findings. Numerous data collection approaches were used which might have overlapped and lead to repetition. For instance, an observed situation might also be found in the incidence log. This limitation could be reduced by checking dates to eliminate double recording. ASTUTE is the final word on security awareness efficacy assessment. It is a first version and clearly needs to be extended and refined as experience in using the mechanism is gained.

Organisations adopting ASTUTE can add any combination of extra measures to the model. Blending different metrics in this way will help to build up a more comprehensive scorecard for effectiveness assessment. Decisions can be made basing on complete overall picture, as opposed to single measures. It is important not to draw incorrect conclusions from assessments. For example, an increase in virus infection rates may be an indicator of staff awareness issues, however, this could also be attributed to issues of with the installed antivirus

software. Likewise, an increase in InfoSec incidents could be indicating issues with awareness of the employees (genuine increase in actual breaches), however, it could also be as a result of improved awareness (employees now understanding the importance of reporting breaches) or even a newly revealed (as yet unpatched) vulnerability. Using a portfolio of measures thus facilitates sense-making in this complex zone.

VIII. CONCLUSION

In conclusion, employees' InfoSec knowledge was very low initially. However, they had a positive attitude towards secure behaviours when handling the organisation's information assets, although they lacked the skills carry out the secure behaviours. This highlights the fact that the risk that employees expose the organisation to may be truly unintentional an a consequence of of naivety [3], [8], [41].

What is disappointing is that although knowledge had considerable positive change during the iterations, attitudinal change remained marginal. This is probably due to employees having a pre-existing attitude towards the organisation, which awareness and training cannot necessarily alter.

Our empirical study confirms that behavioural intentions do not necessarily convert to actual behaviours. Therefore, it is necessary to repeat awareness training until behavioural measures improve. We also demonstrated, with ASTUTE, that it is possible to quantify the efficacy of InfoSec interventions and we hope that organisations will benefit from this proposal.

REFERENCES

[1] M. D. Cavelty, "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities," *Science and engineering ethics*, vol. 20, no. 3, pp. 701–715, 2014.

[2] T. R. Peltier, *Information security risk analysis*. Auerbach publications, 2010.

[3] PWC, "The Global State of Information Security Survey 2015," *Price Waterhouse Coopers*, 2016.

[4] S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of IT security," *Computer Fraud & Security*, vol. 2009, no. 2, pp. 5–10, 2009.

[5] J. Cox, "Information systems user security: A structured model of the knowing–doing gap," *Computers in Human Behaviour*, vol. 28, no. 5, pp. 1849–1858, 2012.

[6] K. Renaud and M. Warkentin, "Using Intervention Mapping to Breach the Cyber-Defense Deficit."

[7] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behaviour," *Computers & Security*, vol. 49, pp. 177–191, Mar. 2015.

[8] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Information & management*, vol. 51, no. 2, pp. 217–224, 2014.

[9] M. Wilson and J. Hash, "Building an information technology security awareness and training program," *NIST Special publication*, vol. 800, no. 50, pp. 1–39, 2003.

[10] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," *Mis Quarterly*, pp. 757–778, 2010.

[11] A. Da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security*, vol. 49, pp. 162–176, 2015.

[12] H. A. Kruger and W. D. Kearney, *Measuring information security awareness: A West Africa gold mining environment case study*. 2005.

[13] L. Drevin, H. A. Kruger, and T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment," *Computers & Security*, vol. 26, no. 1, pp. 36–43, 2007.

[14] S. Egelman and E. Peer, "Scaling the security wall: Developing a security behaviour intentions scale (sebis)," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015, pp. 2873–2882.

[15] R. Wash and E. J. Rader, "Too Much Knowledge? Security Beliefs and Protective Behaviours Among United States Internet Users.," in *SOUPS*, 2015, pp. 309–325.

[16] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, 2014.

[17] J. D. Nosworthy, "Implementing information security in the 21st century—do you have the balancing factors?," *Computers & security*, vol. 19, no. 4, pp. 337–347, 2000.

[18] M. H. S. Peláez, "Measuring effectiveness in information security controls," *SANS Institute InfoSec Reading Room, http://www. sans. org/reading_room/whitepa pers/basics/measuring-effectivenessinformation-security-controls_33398*, 2010.

[19] L. Brunetti *et al.*, "Surveillance of nosocomial infections: a preliminary study on hand hygiene compliance of healthcare workers," *Journal of preventive medicine and hygiene*, vol. 47, no. 2, 2006.

[20] J. Bucher, C. Donovan, P. Ohman-Strickland, and J. McCoy, "Hand washing practices among emergency medical services providers," *Western Journal of Emergency Medicine*, vol. 16, no. 5, p. 727, 2015.

[21] W. Hubbard, "Methods and techniques of implementing a security awareness program," *SANS Institute White Paper, SANS Institute, Bethesda, MD*, 2002.

[22] E. Schwitzgebel and J. Rust, "The behaviour of ethicists," *Blackwell Companion to Experimental Philosophy*, 2016.

[23] J. Thrul, A. Bühler, and F. J. Herth, “Prevention of teenage smoking through negative information giving, a cluster randomized controlled trial,” *Drugs: Education, Prevention and Policy*, vol. 21, no. 1, pp. 35–42, 2014.
[24] H. Zhang, “Cigarette smoking among Chinese medical staff,” *The Lancet*, vol. 385, no. 9978, p. 1621, 2015.
[25] Y. Joshi and Z. Rahman, “Factors affecting green purchase behaviour and future research directions,” *International Strategic Management Review*, vol. 3, no. 1–2, pp. 128–143, 2015.
[26] N. S. Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organisations,” *Computers & Security*, vol. 56, pp. 70–82, 2016.
[27] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, “Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organisational insiders,” *Information & management*, vol. 51, no. 5, pp. 551–567, 2014.
[28] P. Davis, “Measuring the Effectiveness of Information Security Awareness Training,” *Retrieved July*, vol. 12, no. 2014, p. 2014, 2008.
[29] M. Chapple, “Four ways to measure security success,” *SearchSecurity*. [Online]. Available: https://searchsecurity.techtarget.com/tip/Four-ways-to-measure-security-success. [Accessed: 10-Sep-2018].
[30] ENISA, “Information security awareness initiatives: Current practice and the measurement of success,” *ENISA*, p. 24, 2007.
[31] I. Ajzen, *The theory of planned behaviour: reactions and reflections*. Taylor & Francis, 2011.
[32] R. P. Bagozzi and S. K. Kimmel, “A comparison of leading theories for the prediction of goal-directed behaviours,” *British Journal of Social Psychology*, vol. 34, no. 4, pp. 437–461, 1995.
[33] D. F. Galletta and P. Polak, “An empirical investigation of antecedents of Internet abuse in the workplace,” *SIGHCI 2003 Proceedings*, p. 14, 2003.
[34] T. J. Madden, P. S. Ellen, and I. Ajzen, “A comparison of the theory of planned behaviour and the theory of reasoned action,” *Personality and social psychology Bulletin*, vol. 18, no. 1, pp. 3–9, 1992.
[35] P. A. Pavlou and M. Fygenson, “Understanding and predicting electronic commerce adoption: An extension of the theory of planned behaviour,” *MIS quarterly*, pp. 115–143, 2006.
[36] S. Taylor and P. Todd, “An integrated model of waste management behaviour: A test of household recycling and composting intentions,” *Environment and behaviour*, vol. 27, no. 5, pp. 603–630, 1995.
[37] A. Da Veiga and J. H. Eloff, “A framework and assessment instrument for information security culture,” *Computers & Security*, vol. 29, no. 2, pp. 196–207, 2010.
[38] H. A. Kruger and W. D. Kearney, “Consensus ranking–An ICT security awareness case study,” *computers & security*, vol. 27, no. 7–8, pp. 254–259, 2008.
[39] M. Lichtman, *Qualitative research in education: A User’s Guide: A user’s guide*. Sage, 2012.
[40] J. Goo, M.-S. Yim, and D. J. Kim, “A path to successful management of employee security compliance: An empirical study of information security climate,” *IEEE Transactions on Professional Communication*, vol. 57, no. 4, pp. 286–308, 2014.
[41] C. Brodie, “The importance of security awareness training,” 2008.