Lessons Learned from an Organizational Information Security Awareness Campaign

Juan-Marc Scrimgeour, Jacques Ophoff

Lessons Learned from an Organizational Information Security Awareness Campaign

Juan-Marc Scrimgeour and Jacques Ophoff[0000-0003-0634-5248]

University of Cape Town, Cape Town, South Africa
SCRJUA001@myuct.ac.za, jacques.ophoff@uct.ac.za

Abstract. Educating end-users to improve information security awareness plays an important part in securing organizational environments. While best practice standards provide a set of minimum information security awareness controls that should be implemented, little guidance is given on how to implement these controls to ensure the effectiveness of training. This research defined and evaluated a method for implementing an information security awareness campaign (ISAC) within an organization. The method is based on prior research and standards, while assisting the subject in improving their ISAC through the creation of artefacts and measurement techniques. A design science research approach was used with several research cycles to design the method. The method was implemented within an organization and evaluated based on the impact, effectiveness and results of each step, as well as the feedback from participants (two questionnaires were completed by 47 and 36 employees respectively). The research found both positive and negative results. Certain steps within the method proved time consuming and confusing to some participants. Although improvements can be made, the method was found to be adequate as it achieved the required objective within the organization and provided the organization with a risk-based method and visual representation to measure awareness on specific information security awareness topics. The results of the study not only provided value to the organization but provides a validated method for implementing an ISAC which could be applied in other contexts.

Keywords: Information Security Awareness Campaign, Effectiveness.

1 Introduction

Research has shown that educating end-users on information security awareness (ISA) plays an important part in securing your environment [1-3]. ISA can be defined as *"a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure"* [4]. Best practice standards provide a set of minimum controls that should be implemented, however, little guidance is given on how to implement these controls to ensure the effectiveness of the training [2, 5, 6]. The field of ISA is popular; however, most studies focus on improving training or how to implement the training in a different way. There seems to be a lack of studies that focus on how to

implement a campaign that meets the stringent requirements set by best practice standards. In addition, research on effectiveness measurement techniques is largely focused on questionnaires, and as a result, questionnaires are the primary means of measuring effectiveness. However, researchers in this field state that the questionnaire technique can be improved upon by supplementing it with hard measures.

This research defined and evaluated a method for implementing an ISAC within an organization based on existing research and standards, while assisting the subject in improving their ISAC through the creation of artefacts and measurement techniques. The method used attempts to supplement the widely used questionnaire technique with risk management practices, such as those defined by the NIST [4], *"The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation."* This will address the research problem by implementing and evaluating a method for delivering an ISAC within an organization that is measurable and relies on the use of risk management metrics to determine its effectiveness. The current paper reflects on the lessons learned during this ISAC implementation process.

The study was conducted within a financial institution in South Africa. The training provided was created and administered by employees of the target organization (TO) and focused on one specific theme (Acceptable Usage Policy).

2 Background

Recently several studies have focused on identifying the best way to improve on an ISAC. These studies have varied in approach from simulations [5, 7, 8] to the development of educational material [2, 9]. When examining factors which influence the effectiveness of ISA the following themes emerge: the end-user's knowledge and skills, the personality of the end-user, and the environment that surrounds the end-user.

There is little guidance of what knowledge should be passed on in ISA. While some standards (e.g. PCI-DSS) state key focus areas for ISA, it is not all-encompassing and is normally focused on software developers. In addition, it is suggested that the end-user's personality can influence the effectiveness of ISAC. Studies show that end-users tend to interpret, experience, and perceive the importance of ISA differently based on personality [10-12]. These studies, in how personalities can impact the effectiveness of ISA, have highlighted the importance of how one communicates the content and importance of ISA. Lastly, studies show that context is crucial in the effectiveness of ISA training [3, 13, 14]. This aligns with standards and regulations which state that ISA training should be relevant to end-users' role and environment [15, 16]. In addition, it has been shown that demographic factors, such as age and educational level, can affect employee security policy awareness and compliance [17]. Effective training in one environment does not guarantee success in another.

2.1 Measuring the Effectiveness of ISA Training

Two primary measurement techniques can be identified from prior research: technical measures, in the form of metrics (number of reported phishing mails; incidents due to change, data leakage events, audit findings); and questionnaires or surveys, that test the knowledge of end-users.

Technical measures of effectiveness are seldomly reported in academic publications, in most part because obtaining the data required from businesses has proven difficult (if not impossible) as the data owners have security concerns around sharing the data [18, 19]. Most studies that make use of such measures are case studies using simulated phishing campaigns [5, 8, 9]. In addition, it has been seen that methods also include reporting on incidents, testing employee pre and post training, and collection feedback from stakeholders [20]. While these studies show that end-users are retaining what they have learnt and have changed their behavior, it only addressed one security concern, albeit an important one. On the other hand, questionnaires are by far the most popular means of measuring the effectiveness of ISACs, with more than three-quarters of studies performed over the past years focusing on the designing and using a variation of a questionnaire to test end-user knowledge of ISA topics. While many questionnaires are self-developed they should ideally be grounded in best-practice. For example, a formal approach is taken by Poepjes [19], which bases questions and focus areas on the ISO 27001/2 standard.

2.2 ISA Capability Model

The Information Security Awareness Capability Model (ISACM) [19] requires that several metrics be obtained to determine what awareness campaigns need to be delivered in the environment. These metrics are Awareness Importance (AI), Awareness Capability (AC) and Awareness Risk (AR). AI is derived from taking an information security best practice standard, extracting the controls and rating their level of importance regarding user awareness of the control within the environment. AC is derived from surveying a random sample of end-users on their understanding of the various controls identified as important in the AI phase. AC can therefore be defined as the end-users' understanding and knowledge around specific awareness controls. AR is then calculated by applying the values obtained to an awareness risk matrix. This matrix is used to determine the AR rating. AR can therefore be defined as the risk identified when comparing the users' AC against the AI score for each awareness control. The results of the ISACM can be used to create a targeted and measurable ISAC.

3 Implementation Methodology

We created a practical method to implement an ISAC, derived from the ISACM. The method adapted the model to the environment of a target organization (TO). Several instruments were developed in conjunction with TO personnel:

- Control framework: the control framework is a list of information security best practice controls. The framework aligns with the information security framework (ISF) that the TO uses.
- Control awareness survey: the survey contains questions to determine the AC value of controls that received an AI rating of *moderate* to *extremely important*. The survey should be updated upon any change in the control framework.
- Awareness risk matrix: this matrix is used to determine the AR rating and was adapted from the TO risk framework.

Fig 1 shows how the instruments and metrics were combined in a step-wise approach.

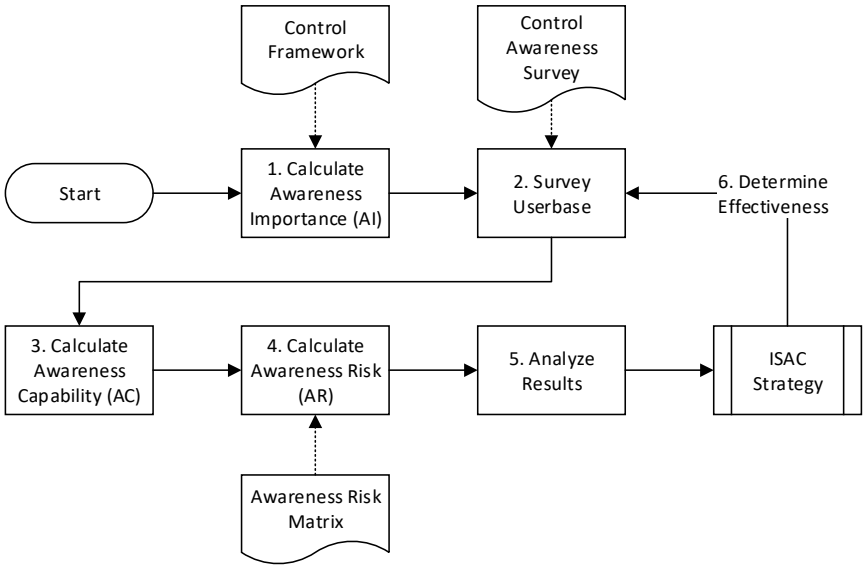

Fig. 1. ISAC Methodology

3.1 Awareness Importance (AI)

The control framework is a list of information security best practice controls which will be given to Senior Staff members of the IT security department that are stakeholders in the ISAC. Each control is then rated by the IT security team to determine the AI of each control, for each end-user group. The control framework is developed by incorporating the IS/cybersecurity framework of the TO. The NIST [4] defines a cybersecurity framework as "a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes".

3.2 Survey Userbase

The control awareness survey is dependent on the results of the control framework. To not overburden users only the top ten controls, that are deemed *moderate* to *extremely important* for each group, are used in the survey. Additionally, the questions are tailored to the identified group's environment. The results of the survey are used to calculate the group's AC.

3.3 Calculate Awareness Capability (AC)

The results of the survey are then used to obtain an average score for each control for each group, used as the AC metric. For example, for control X, the survey results for 10 users from group Y are 2, 3, 2, 4, 5, 2, 2, 4, 5 and 2. The scores are added together, resulting in a total of 31 out of 50. This is then divided by 10 (the number of participants) to give an AC score for control X and group Y of 3.1.

3.4 Calculate Awareness Risk (AR)

The awareness risk matrix must be applied in the TO environment so that it aligns with the organization's risk framework. This results in an awareness risk matrix that will be used to plot the AI and AC scores, to determine the AR score for each control.

3.5 Analyze Results

The AR rating for each control will be used to determine what training should be implemented in the environment for each user group. The control with the highest AR will be used to compile and implement the ISAC strategy for the coming training period. The ISAC strategy is then implemented by the information security team.

3.6 Determine Effectiveness

Once the training curriculum addressing the AR has been successfully implemented and is considered complete by the information security team, the same questionnaire that was used to measure AC will be sent to a new sample set of users for each target group (i.e. it does not contain any of the users that answered in the original sample group). The answers from the second sample group will then be reflected on the awareness risk matrix. Should the userbase have learnt anything from the ISAC, their AC score will be higher, therefore reducing the AR score. As the AR score of a control reduces, a new control with a higher AR score will become the new focus for the next ISAC period.

3.7 Target Organization Overview

The TO is required by both regulation and legislation to implement ISA within their environment, with the objective to change the behavior of staff to be more security

minded. The TO is aligned with international best practices and has chosen the Information Security Forums Standards of Good Practice (SoGP) [15] as their primary ISF. The responsibility of implementing training within the TO is given to the IT security department where there are multiple security teams, including: information security, cyber security, and access control, to name a few. Senior members of the various teams within the IT security department form part of the ISAC stakeholder group.

The TO is required by their board of directors to deploy at least four topics a year, allowing topics to be deployed every three months at a minimum. Training is deployed in multiple ways depending on the level of training or awareness the information security team needs to implement. For structured e-learning style training, the information security team makes use of a learning management system, which deploys the training to the end-user and tracks their progress and completion status. E-learnings are either sourced from an external supplier who is an expert on the topic or created internally by the TO's human resource employee education department that specializes in educating staff, with the information security team playing the role of the subject matter expert.

4 ISAC Implementation and Lessons Learned

The method was implemented and evaluated in a financial institution in South Africa over a ten-month period in 2018 (January to October). Ethical clearance from the university and permission from the organization was obtained before any data was collected. Implementation and evaluation data were collected in several ways. The first collection method was in the form of artefacts created in Microsoft Excel to capture the responses of the IT security team in a structured manner. The second method was a questionnaire that was sent to a group of end-users to obtain the participants' understanding of the material given to them. The content was obtained from documents and questionnaires previously created by the TO. Lastly, feedback regarding the method's efficacy was collected through observation by the researcher as well as from the IT security team; the team members were asked two questions: *"In your opinion, what worked well?"* and *"In your opinion, what did not work well?"*. During the research process we endeavored to minimize bias by using established frameworks and questionnaires, discussing preliminary findings for alternative explanations, and being open to contrary evidence. We are confident that bias was sufficiently considered and that the research was conducted to a high ethical standard.

4.1 Awareness Importance (AI)

The control framework is a list of information security best practice controls which was given to senior staff members of the IT security department that are stakeholders in the ISAC, to measure AI. The control framework aligns to the 2016 version of the SoGP, as the 2018 version [16] was not published until later in the year. The instrument is an adaptation of the instrument used by Poepjes [19]. The stakeholder will rate the AI on a 1 to 5 ordinal scale, with 5 being the highest level of importance.

Data for the control framework was collected by the researcher, with assistance from the information security team. The target audience for the control framework were senior members of the IT security department who are stakeholders in the ISAC. By answering the control framework, these senior members will provide the information security team with their individual understanding of what training is important for each target group (senior management, branch staff, privileged users, contact center and end-users).

The data was collected by sending the control framework to each senior IT security department team member with instructions on how to complete it. Each senior IT security department team member was given two weeks to complete the task. After three months of project prioritization sessions, the control framework was completed by all senior IT security department team members. As an example, Table 1 highlights the top six topics for the end-user group.

Table 1. AI for end-users

SoGP 2016 Controls	Average Score
PA2.5 Portable Storage Devices	4.3
SM1.2 Acceptable Use Policies	4.2
BA2.2 Protection of Spreadsheets	4.2
PA2.4 Employee-owned Devices	4.0
PM2.2 Security Awareness Messages	3.8
IM1.1 Information Classification and Handling	3.8

Lessons learned. Using TO's ISF proved to be very effective, as IT security staff were already familiar with the topics and controls within the framework. As the TO strives to comply with this framework, it meant that most controls within the framework were implemented already. While the translation of this standard into a questionnaire was detailed and comprehensive, determining AI proved to be very difficult, as interpreting the importance and impact of a control can be subjective. Additionally, the length of the control framework proved to be a challenge, as the time taken to complete the AI rating resulted in a slow response rate from participants.

Additionally, participants had various degrees of understanding about the SoGP controls. While the information security team believed that all IT security department team members were familiar with the standard, this was not the case, with some participants struggling to understand the control on its own, how one control differentiates from another, or how the control changes and applies depending on the stakeholder group.

Their seemed to be a difference of opinion about the grouping of stakeholder groups with one participant stating that *"The one thing that really worked well was using the ISF framework to map out areas that needs to be addressed in the different classes of users. Identifying the user classes and applying what is relatable for them from the ISF framework, ensures that all the areas are covered for the correct audience."* While another participant stated that the groupings were inaccurate *"There*

should only be a grouping of three user categories – Senior Management, Privileged users and End-Users. I think although only certain controls might be applicable to certain environments or grouping of users in a certain org [organization] structure it is imperative that the business users as a whole should be made aware of all kinds of risks and attacks a business might face."

A suggestion for improving this step would be to create ISA control groups that are mapped to the ISF. For example, many of the controls, such as data protection controls, were grouped together by the respondents and received similar, if not the same, AI score. A grouping under a control named Data Protection can represent all data protection controls, allowing for one control to supplement many of the smaller controls. This will not only shorten the length of the control framework but allow for more control variety within the various ISACs throughout the year. Additionally, this will provide a single ISAC with multiple topics (each information security control broken up into its smaller ISF controls) as well as make it easier to incorporate other ISFs to the proposed method. The grouped controls would also allow for a more generic definition of a control making it easier for participants not familiar with the ISF of the organization to answer the control framework.

4.2 Survey Userbase

While the information security team was awaiting responses on their AI control framework, the information security team started working on creating questions for the AC questionnaire based on each topic within the SoGP. The information security team were provided several artefacts to assist in crafting these questions that included: the HAIS-Q [21], questionnaire guidelines; and the AI control framework for formatting. The information security team first attempted to create Likert style questions for each topic within SoGP, which proved to be far more challenging than they expected. While theme-specific questions are easily incorporated into Likert style questions, the topics presented in SoGP were far more complex in nature and did not allow for a strongly agree to strongly disagree Likert scale format.

The information security team therefore decided to create questions that were aimed at current processes and procedures in the environment that relate to the SoGP controls. Due to several security incidents and projects throughout the environment, several ISA topics were required to be implemented as a matter of urgency, but conflicted with the topics that were identified in the AI results. It was decided by the TO that they would therefore use the AI results to define the topic for one specific target group, the end-user group. The remaining target groups will receive training based on the current need from the business. While this was not ideal, the risk of not performing the required training for the other target groups was too great to ignore.

The information security team creating the AC questionnaire was informed of the decision and immediately started focusing on delivering the questions that were required for measuring the AC of the top ten topics (out of 132) [15] for the end-user target group. The team created five questions for each topic, which was set up on Survey Monkey. An invitation with a link to the survey was emailed to a random sample of users. Users were given two weeks and a total of 47 users successfully

completed the questionnaire. The information security team felt that this was enough to proceed to the next step. The challenge of competing for employee attention has also been noted in other ISA training contexts [20].

Lessons learned. Using the results from the AI questionnaire to build a questionnaire targeting the end-users proved to have many challenges. The mapping of the ISF controls to general ISA questions or previously used questions from academic papers was near impossible. This resulted in the information security team having to create the questions themselves, as opposed to relying on past research. While the time taken to build this questionnaire took far longer than expected, the resulting questions can be easily used again in the future with little to no rework.

4.3 Calculate Awareness Capability (AC)

Table 2 shows the average score received from the questionnaire. Score ranges from 0 to 5. With a score of 5 meaning the users answered all questions correctly and 0 meaning the user did not answer any of the questions correctly, for that topic. The results show that the end-user target group is unfamiliar with several security controls within their day to day working environment, particularly information classification and handling and the processes and procedures defined in the Acceptable Use Policies (AUP). The sores in Table 1 and 2 is then used to map to the awareness risk matrix to determine the AR score for each control.

Table 2. AC for end-users

SoGP 2016 Controls	Average Score
IM1.1 Information Classification and Handling	1.7
SM1.2 Acceptable Use Policies	1.9
BA2.2 Protection of Spreadsheets	2.4
PA1.2 Office Equipment	2.4
PA2.4 Employee-owned Devices	2.7
PA2.3 Mobile Device Connectivity	3.1
IM2.2 Sensitive Physical Information	3.2
PM2.2 Security Awareness Messages	3.2
IM1.2 Information Privacy	3.4
PA2.5 Portable Storage Devices	3.5

Lessons learned. The information security team felt the results were a true reflection of the environment with one member of the information security team stating *"The one thing that really worked well was using the ISF framework to map out areas that needs to be addressed in the different classes of users. Identifying the user classes and applying what is relatable for them from the ISF framework, ensures that all the areas are covered for the correct audience."*

4.4 Calculate Awareness Risk (AR)

The TO makes use of an organization-wide risk framework that is developed by the risk management business unit and approved by the board of directors. It examines two main dimensions, impact and likelihood. For the organization impact holds greater value than likelihood, as the TO sees any impact within the short term (three years) as being significant enough to warrant attention.

The strategy applied by Poepjes [19] is then applied to this matrix, supplementing likelihood with AC and impact with AI. The result of mapping aggregated scores for AI and AC for each grouping will be an AR rating for each control. The AI and AC scores for the end-user target group were then mapped on the awareness risk matrix. Fig 2 demonstrates the AI and AC mapping.

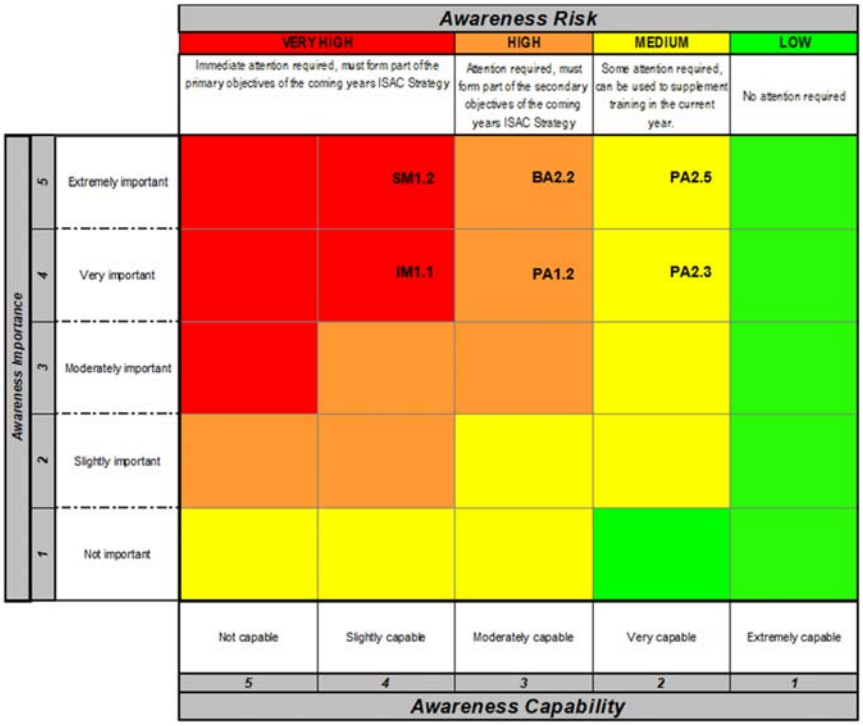

Fig. 2. End-user awareness risk matrix

The AC score is inverted to map to the risk matrix. This is done by taking the highest rating and subtracting the current score. For example, “IM1.1 Information Classification and Handling” received an AC score of 1.7 in Table 2, which is subtracted from the highest risk rating of 5, to give the risk matrix AC mapping of 3.3. On the risk matrix the area towards the top left indicates very high risk. Controls in this area require immediate attention and should form part of the primary objectives of the next

ISAC strategy. As can be seen “SM1.2 Acceptable Use Policies” and “IM1.1 Information Classification and Handling” are identified as very high risk for the organization.

Lessons learned. The plotting of the results of the AI and AC questionnaire provided a very effective means of illustrating the AR within the environment. Unfortunately, the 5x5 risk matrix results in groups of ARs, requiring the information security team to revert to the raw data to determine the highest AR. Additionally, the awareness risk matrix required the original AC score to be inverted to map to the awareness risk matrix. While this did not affect the results of the AR score, it was an unnecessary complication in an otherwise well-developed step.

4.5 Analyze Results

The results from mapping the AI and AC score showed that the largest AR score comes from the topic *“SM1.2 Acceptable Use Policies”*. The information security team agreed that this reflects what they had suspected and used this topic for the ISAC. The information security team then started building an ISAC strategy to increase end-users’ awareness of AUP controls within the environment.

ISAC Strategy. The team had multiple discussions with various vendors and departments to determine the best way to deliver training for this topic. Due to the topic being organization-specific, generic e-learnings from vendors proved to be inadequate. Recommendations from the human resources employee education department within the organization required creating a very lengthy and complex, custom built, e-learning. This too was deemed inadequate, as the team knew from prior training efforts that lengthy e-learnings do not have a high completion rate.

The information security team decided to focus on an awareness campaign with the overall theme of *“Protecting the family”*. The theme was chosen because it aligned with a family-focused product which the organization was rolling out, as well as the organizational culture (communications often referred to ‘our family’ and ‘being part of a great family’). The goal was to instill a security mind-set and a sense of responsibility in employees.

To implement the campaign posters and desktop backgrounds (wallpapers) were designed. Large (A3) posters were displayed in social areas in every building. These posters were intended to be eye-catching, with minimal text but reference to where employees could go to find out more. Smaller (A4) posters were placed behind every bathroom stall door and contained more detailed information. The desktop backgrounds also had minimal text but provided the user with the central call-to-action and link to more information.

The information security team then created a series of emails in line with the style of the posters, with the content being only a few short paragraphs. An email was sent out every two weeks, each tackling a different section of the AUP. The topics were: sharing data, laptop security, policy document awareness and importance, communicating security risks, removable media, backups and shared drives, and disposing of information. Content was in plain English and could be read in under three minutes.

Lessons learned. The visual representation of the AR within the environment made identifying the required training very easy. The information security team felt that it was a true reflection of the current environment, with one member of the information security team stating: *"One could gain a true direction for awareness training within an organization"*.

Building the ISAC strategy proved to be quite challenging, due to the nature of the topic chosen. As the topic focused on AUP, the training needed to be customized to the environment, making it impossible to use generic training from a third party proficient in the topic. While the content was easy for the team to come by, as it came from a company policy, deciding on the method to deploy the training was not. The chosen method was a series of emails supported by a marketing campaign. The information security team could benefit from previous research, such as that done by Pattinson et al. [12], to determine what method of training is best suited for different end-users.

4.6 Determine Effectiveness

Once the information security team had deployed the training to their satisfaction, the questionnaire and email was sent to a further 255 respondents. Respondents were given three weeks to complete the survey with a reminder e-mail sent a week before final closure date. A total of 36 users successfully completed the questionnaire.

The average score received from the second questionnaire show that there was a slight increase (from an average score of 1.9 before training to 2.5 after training) in the user's knowledge of the security controls within their day to day working environment. The original AI and post training AC score for the end-user target group was then mapped on the awareness risk matrix. There was a clear move of AC to the right (more capable), making the AR decrease from a very high risk to a high risk.

Lessons learned. Re-performing the survey, as well as calculating the new AC and AR scores was done significantly faster than many of the other steps. The artefacts created at the start of this method made this step very efficient.

The move of the AC of the target group from very high to high proved to be a very effective illustration of the effectiveness of the training implemented. The information security team believed that the method used to train the staff was not the most effective but believed that the slight move was an accurate view of the effectiveness of the ISAC and were therefore pleased with the results.

5 Conclusions

While we acknowledge the limitations of statistical generalization within a single case study we propose that analytic generalization is possible. Such lessons learned may potentially apply to a variety of contexts. Our study reflects on the practical steps required in an ISAC and the hurdles staff who implement it will have to overcome. These include identifying and prioritizing training topics, creating training material, and effectively measuring learning.

Several limitations should be considered in this study. The TO comes from a highly regulated industry, which requires compliance with many controls. This requirement drives some of the decision-making in this case. Due to compliance requirements and risks prevalent in the environment, the method was only used on a single target group that was considered less risky by the TO. The implementation of this method over a longer period would provide the opportunity to not only collect more data but help improve and evolve the method. Additionally, the content and mechanisms used to deliver training was decided on by TO staff. While TO staff were sure of its effectiveness as a training delivery method, there is no evidence to validate their assumption, other than their experience in the field and knowledge of the environment.

While our study contributes to the validation of the model proposed by Poepjes [19] it also indicates the need for further research. Within the field of ISA training ways to efficiently measure the effectiveness of a campaign are needed. Further research could also investigate the methodology used to conduct the training, and how this impacts the effectiveness of the ISAC. Additionally, the incorporation of hard measures, such as phishing simulation results and other user behavior metrics, could prove effective but more research is required on what those hard measures should be.

Acknowledgements. This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

References

1. Daniel Ani, U.P., He, H.M., Tiwari, A.: Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity. pp. 169–182. Springer International Publishing (2016).
2. Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. Presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (2013). https://doi.org/10.1145/2508859.2516753.
3. Yildirim, E.: The Importance of Information Security Awareness for the Success of Business Enterprises. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity. pp. 211–222. Springer International Publishing (2016).
4. National Institute of Standards and Technology: Glossary | Computer Security Resource Center, https://csrc.nist.gov/glossary/.
5. Aloul, F.A.: The Need for Effective Information Security Awareness. JAIT. 3, 176–183 (2012). https://doi.org/10.4304/jait.3.3.176-183.
6. Stewart, G., Lacey, D.: Death by a thousand facts: Criticising the technocratic approach to information security awareness. Info Mngmnt & Comp Security. 20, 29–38 (2012). https://doi.org/10.1108/09685221211219182.
7. Arachchilage, N.A.G., Love, S.: Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior. 38, 304–312 (2014). https://doi.org/10.1016/j.chb.2014.05.046.
8. Young-McLear, K., Wyman, G., Benin, J., Young-McLear, Y.: A White Hat Approach to Identifying Gaps Between Cybersecurity Education and Training: A Social Engineering

Case Study. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity. pp. 229–237. Springer International Publishing (2016).
9. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D.: Managing information security awareness at an Australian bank: a comparative study. Info and Computer Security. 25, 181–189 (2017). https://doi.org/10.1108/ICS-03-2017-0017.
10. Kajzer, M., D'Arcy, J., Crowell, C.R., Striegel, A., Van Bruggen, D.: An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security. 43, 64–76 (2014). https://doi.org/10.1016/j.cose.2014.03.003.
11. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M.: Individual differences and Information Security Awareness. Computers in Human Behavior. 69, 151–156 (2017). https://doi.org/10.1016/j.chb.2016.11.065.
12. Pattinson, M., Butavicius, M., Ciccarellol, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A.: Adapting Cyber-Security Training to Your Employees. In: Clarke, N. L. & Furnell, S. M. (ed.) Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance. pp. 67–79. University of Plymouth (2018).
13. Tsohou, A., Kiountouzis, E., Karyda, M., Kokolakis, S.: Analyzing trajectories of information security awareness. Info Technology & People. 25, 327–352 (2012). https://doi.org/10.1108/09593841211254358.
14. Waly, N., Tassabehji, R., Kamala, M.: Improving Organisational Information Security Management: The Impact of Training and Awareness. In: 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems. pp. 1270–1275 (2012). https://doi.org/10.1109/HPCC.2012.187.
15. Chaplin, M., Creasey, J., & Thathupara, S.: The standard of good practice for in-formation security 2016. Information Security Forum Limited (2016).
16. Jordan, A., Haken, G., & Creasey, J.: The Standard of Good Practice for Information Security 2018. United Kingdom: Information Security Forum (2018).
17. Chua, H.N., Wong, S.F., Low, Y.C., Chang, Y.: Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics. 35, 1770–1780 (2018). https://doi.org/10.1016/j.tele.2018.05.005.
18. Lebek, B., Uffen, J., Breitner, M.H., Neumann, M., Hohler, B.: Employees' Information Security Awareness and Behavior: A Literature Review. In: 2013 46th Hawaii International Conference on System Sciences. pp. 2978–2987. IEEE, Wailea, HI, USA (2013). https://doi.org/10.1109/HICSS.2013.192.
19. Poepjes, R.: The development and evaluation of an information security awareness capability model: linking ISO/IEC 27002 controls with awareness importance, capability and risk, https://eprints.usq.edu.au/28067/, (2015).
20. Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S.: An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. In: 51st Hawaii International Conference on System Sciences, HICSS 2018, Hilton Waikoloa Village, Hawaii, USA, January 3-6, 2018. pp. 1–10 (2018). https://doi.org/10.24251/HICSS.2018.635.
21. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security. 42, 165–176 (2014). https://doi.org/10.1016/j.cose.2013.12.003.