An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations

Moneer Alshaikh, Sean B. Maynard, Atif Ahmad and Shanton Chang
School of Computing and Information Systems
The University of Melbourne
Sean.Maynard@unimelb.edu.au

Abstract

Effective information security training and awareness (ISTA) is essential to protect organizational information resources. Our review of industry best-practice guidelines on ISTA exposed two key deficiencies. First, they are presented at a conceptual-level without any empirical evidence of their validity. Second, the guidelines are generic (one size fits all) without consideration of the diversity in organizational contexts where they will be applied. Given these deficiencies in ISTA guidance, this paper reports on the findings of an exploratory study into how ISTA is implemented in different organizational contexts in six organizations. The paper identifies three challenges: the lack of motivational aspects in current ISTA program, the competition for employees' attention and the difficulty in measuring the effectiveness of ISTA program. Several recommendations and suggestions were outlined to overcome these challenges.

1. Introduction

Organizations expend a considerable amount of money and resources in information security. Despite this, the number of incidents reported is still on the increase. Recent security reports show that a significant proportion of non-malicious cybersecurity breaches are caused by employee noncompliance with the organization's information security policies [1]. For example, current employees are reported to be responsible for over 50 percent of reported security breaches [2]. The noncompliance of employees to organizational security policies is a major organizational concern [3]. Whilst policies state how employees should deal with email links etc., many incidents are still being caused by employees, through carelessness or poor security behaviour in response to phishing (e.g. leading to malware penetration of systems resulting in leakage of trade secrets and intellectual property or the disruption of mission-critical systems)[4, 5]. Examples of these types of non-malicious incidents are common. In 2016, a staff member from a government organization clicked on an Australia Post themed email which infected the workstation with ransomware (Cryptolocker). It encrypted the files on a computer asking for a "ransom" of $US300 to be paid in virtual currency bitcoin[6].

Security researchers have consistently argued that information security training and awareness (ISTA) programs should be in place to raise employees' awareness of security risk, and provide them with the required skills and knowledge to comply with security policy [7]. Although organizations adopt and employ ISTA programs to educate users, there is still an increase in the number of security non-malicious breaches as a result of employees' noncompliance with security policy [8]. This trend may indicate that many current security training and awareness programs are not as effective as they should be.

Therefore, there is a need to investigate current practices that are implemented by organizations to manage their ISTA programs. The aim of this paper is: (1) to explain how ISTA management practices are implemented in various organizational contexts; and (2) to identify the challenges and issues that organizations face during the implementation of ISTA. The study addresses the following research question:

How is information security training and awareness implemented in organizations?

This paper is organized as follows. First, best-practice industry guidelines on ISTA are reviewed in the background section. Second, the methodology employed in this research is explained. Third, the findings of the exploratory study are reported. Fourth, an analysis of the findings is conducted. Finally, we conclude with implications of the research.

2. Background

There is consensus in the literature on the need for organizations to develop ISTA programs to protect their information assets [9, 10]. Existing information security management frameworks integrate the ISTA program with other security functions such as: security policy, risk management and incident management [11-14]. For example, ISO/IEC 27002 stresses the need for ISTA programs, recommending that "all employees

URI: http://hdl.handle.net/10125/50524
ISBN: 978-0-9981331-1-9

of the organization should receive appropriate awareness, education and training and regular update in organizational policies and procedures, as relevant for their job function" [15].

In the literature, the ISTA program is sometimes referred to as security education, training and awareness (SETA)[16]. The literature distinguishes between education, training and awareness in terms of their aim, level and target. Whitman and Mattord [17] suggest: *education* is for security professionals to build in-depth knowledge around the design and implementation of a security program; *training* provides employees with an adequate level of skills to enable them to perform their job securely; and *awareness* involves providing general employees with information and informal training to raise their awareness about risk and security. As practices and activities undertaken in organizations usually fall under the training and awareness definitions, while education is typically done in specialized security education institutes and universities [18], we adopt the term information security training and awareness (ISTA) throughout this paper.

The importance of an ISTA program in safeguarding information assets has led many authors to recommend establishing programs within organizations as part of their overall security strategy [19, 20]. There are several guidelines for organizations developing ISTA programs [7, 17, 21, 22]. These approaches can be summarized across three types of generic management activities: (1) *development,* (2) *implementation* and (3) *evaluation*. The following discussion uses these three activity types to discuss existing approaches and models for developing ISTA programs.

The development phase includes activities used to understand the current organizational situation, obtain management support and acquire resources to develop an effective program [23, 24]. These activities include conducting a needs assessment for an ISTA program (which may include legislated requirements), defining goals and objectives, establishing the ISTA development team, and identifying the target audience for an ISTA program. The literature discusses the importance of understanding the needs of an organization and the design ISTA programs that meet these specific needs. For instance, Peltier [25] contends that an effective ISTA program should consider the needs and current level of training and awareness, and have a sufficient understanding of the target audience of the program. Similarly, Valentine [26] proposes an ISTA program that begins with an assessment phase followed by identification and education phases. In terms of setting goals and objectives, researchers stress the importance of defining achievable and measurable goals and objectives for the ISTA program [27]. Development phase activities also include developing materials for ISTA consisting of tasks around topic selection and material creation [28].

The Implementation phase focuses on the conduct of the ISTA program using a variety of delivery methods. The literature on the implementation of the ISTA discusses methods of effectively delivering ISTA messages. Several authors recommend the use of a combination of methods for delivery, such as newsletters, email, note-taking tools to aid memory (e.g. pens and notepads), and posters that expose those within the organization to convey the security messages on consistent and ongoing bases [25, 29].

The final ISTA phase is evaluation, where the organization reviews and evaluates its ISTA initiatives to measure their effectiveness. Effectiveness is usually measured through identifying changes in employee behaviour that impact information security [19]. Existing approaches focus on evaluating the knowledge obtained for the program [30]. This is a very limited view of evaluation. Evaluation should also focus on the effect of ISTA on the overall security of the organization because of the change in employee behaviour [31]. One way to measure the effectiveness of ISTA is to compare the incidence of noncompliance-related security events before and after implementation of the ISTA program.

Our review of the literature found that existing guidelines and best practice standards do provide recommendations for organizations on how to develop an effective information ISTA program. However, these guidelines and standards are: (1) conceptual and lacking support from empirical data, and (2) generic in nature and do not consider the organizational context. Further, implementing the recommended practices from the standards does not guarantee their quality in practice [32].

In practice, we know very little about how organizations manage their ISTA programs and how well they implement the managerial practices associated with ISTA. Therefore, there is a need to investigate the current state of the management process of ISTA programs. This study addresses this gap in the literature and provides a more rigorous and comprehensive understanding of the practices of ISTA and how well they are implemented in organizations.

3. Research Methodology

A qualitative and exploratory research approach was adopted to enable the researcher to gain an in depth understanding the research phenomenon. It consists of six semi-structured interviews with senior and middle level management ISTA experts (see Table

1). The interviewees were chosen for their level of experience in the area. The questions were aimed at investigating how these experts implemented their ISTA programs within their organizations. The interviews lasted approximately 60 minutes on average. Participants were asked to describe the activities they undertake to manage the organization's ISTA program. Participants reported on their current organizations, but also mentioned their experience from past organizations, giving more data on diverse types of organizations. Participants were asked follow-up questions via Email where required. The participants come from different organizational size and industry.

Table 1. Background study participant details

ID	Role	Industry	Years of Experience
CISO1	Chief Information Security Officer	Government	15+
Mng1	Security Manager	IT Services	5+
Mng2	Senior Security Manager	Insurance	20+
CISO2	Chief Information Security Officer	Automotive	10+
Mng3	Security Awareness Manager	Banking	10+
Mng4	Security Awareness Manager	Banking	9+

4. Findings

A qualitative data analysis approach was adopted in this study as per [33]. The interviews were transcribed from audio recording and detailed analysis was undertaken to gain an understanding of what managerial activities the participants undertake as part of their jobs. This resulted in approximately 80 pages of transcribed text. The collected data was coded sentence-by-sentence to identify themes. The grounded theory analysis technique was employed to analyse the data. A coding process consisting of open, axial and selective coding was used to identify themes related to how an ISTA program is implemented in organizations. Four themes were identified: ad-hoc vs. formal approach to ISTA activities, lack of motivational aspects in ISTA programs, competition for employees' attention and difficulty to measure the effectiveness of the ISTA program. This section presents evidence related these four themes.

4.1 Ad-hoc vs. Formal ISTA Activities

The findings of this study provided insight on how ISTA activities are conducted in organizations. The data shows the differences between ad-hoc and formal approach that organizations adopt to the implementation of six key ISTA activities: identify ISTA program needs, develop ISTA program plan, establish ISTA program development team, develop ISTA materials, conduct ISTA program and review ISTA program.

4.1.1 Identify ISTA Program Needs. Identify the needs for ISTA Program is one of the key practices that has been reported by the participants. The formal approach to this practice involves using various inputs to identify the needs. Mng1, CISO2, Mng3 and Mng4 reported that policy, incident reports, risk assessment, threat intelligence, and users' feedback are used to identify the needs for ISTA program. For instance, Mng4 stated: *"There are numerous inputs. Understanding the threat landscape: what is currently happening or what's being advertised. There's also a component around what incidents have we seen in the past, be they to our organization or to other industries or organizations. we also look at what user feedback we are receiving. If people are actually saying that these are their concerns--these are their issues, we'll also feed that into it, as well. Then, also, the strategic direction of where the ISO wants to build capability. That will really dictate more or less the key areas."*

In the ad-hoc approach, organizations only use policy to identify the needs. CISO1 and Mng2 stated that in their organizations only policy is used as an input to identify the needs for ISTA.

4.1.2 Develop ISTA Program Plan. While all the six participants acknowledge the importance of planning for ISTA, the extent to which planning is formalized depends on the circumstances and the characteristics of the organization. CISO2, Mng3 and Mng4 stated that there are thorough planning activities, covering long term (strategic) and short term (tactical) aspects of ISTA. Mng3 stated: *"we set objectives for short campaigns, 'security and fraud week' is developed to achieve specific objectives. We also have very high-level objectives that we'd like to achieve for the overall ISTA program"*

Mng1, Mng2 and CISO1 reported that their organizations tended to take an ad-hoc approach for ISTA planning. They reported that there is some planning, however, it is neither comprehensive, nor formal. Planning covers a few high-level elements such as scheduling of activities. Mng2 stated that, *"We don't have a formal plan for the program, we just have schedule for activities, but it needs improvement"*

This variation can be contributed to the maturity and size of the organization as well as aspects of management support and the availability of resources (including time and personnel).

4.1.3 Establish ISTA Program Development Team. All participants agreed that the delegation of roles and responsibilities around ISTA is a key activity. Organizations that implement ISTA in a formal approach usually have a dedicated team for ISTA. Half of the participants stated that they have a formal team consisting of three to four members. Mng1 states: *"There is a team responsible for security training and awareness. They have the responsibility to create the training material, publishing it on the CBT learning portal. And tracking completion"*.

Organizations that implement ISTA activities in an ad-hoc approach do not have a dedicated team and responsibilities for ISTA are undertaken by members of the organization's security team. CISO1 stated: *"At my last organization, [Bank], we had a team called the learning and development team. They were responsible for managing all CBT or classroom based training. […] but in my current organization, we don't have learning and development unit"*.

CISO1 further provided justification for not having dedicated team in his organization. He stated that because the size of his organization is small, it does not have a dedicated team for ISTA: *"That is probably more of a reflection of the size of our organization. We are not quite big enough to have a dedicated team to this task"*.

4.1.3 Develop ISTA Materials. The study participants agreed that developing ISTA materials is an essential practice which they undertake as part of their role in managing ISTA. Only respondents from organizations that implement ISTA in using formal approach reported the involvement of stakeholders in the development of ISTA materials. Once materials are developed, they are shared with representative stakeholders to review and provide feedback. For instance, Mng3 and Mng4 stated that they solicit input from stakeholders during the development of ISTA materials: *"we create the material and send it to the stakeholders, and then we ask them to provide feedback on the materials, revise it, and publish it"*. After feedback is received and incorporated, the material will be ready for use as part of the organization's ISTA program.

On the other hand, organizations that implement ISTA activities using an ad-hoc approach did not report any involvement of stakeholders.

4.1.4 Conduct ISTA. Respondents from organizations that implement ISTA using an ad-hoc approach reported that they only conduct mandatory security training for all employees using computer based training (CBT). CISO1 reports: *"we have mandatory online training that everyone must complete"*.

Organizations that follow a formal approach, however, implement several types of ISTA program training besides mandatory online training. These ISTA types include ongoing awareness campaigns, training for specific groups/ teams and an intensive awareness campaign over a day or a week. CISO2 reports: *"every month we have awareness messages which comes in the form of email or poster"*. Mgr3 also comments: *"we have a focused security awareness program for specific employees. For example, in my job at the Banking sector, we have specific ISTA programs for call centre people"*. Mng4 also states: "*we have an annual security awareness week. That's run right across the group"*.

4.1.5 Review ISTA Program. Organizations that use a formal approach to review the ISTA program use various techniques to check the effectiveness of their ISTA such as (1) measuring security awareness indications (i.e. the number of reports of security incidents and number of incidents from threats addressed in the ISTA program), (2) Performing phishing simulations, (3) Testing the knowledge of employees prior to, and subsequent to, training, (4) Conducting internal and/or external audits for the ISTA program. Organizations that implement ISTA using an ad-hoc approach did not report activities to measure the effectiveness of their ISTA program. They only relied on statistics generated by CBT software that relate to the number of employees who completed the training and how many times they have undertaken this type of training. Information about completion rates of CBT was used to show managers and auditors (internal and external) that the organization has fulfilled compliance requirements.

4.2 Lack of ISTA Motivational Aspects

The ISTA literature outlines that an effective ISTA program should consist of three main aspects: knowledge, motivation and attitude. These three aspects are vital to change the employees' behaviour towards information security and therefore protect organizations from insider threats caused by employees' noncompliance with security policies. However, a finding of this study indicates that ISTA programs in many organizations focus on only providing knowledge about security whilst overlooking how to improve employee motivation towards security.

The study participants stated that, from the organizational perspective, their ISTA programs have no motivational aspects and are only seen as a compliance requirement that is mandatory for every employee to undertake once a year. Mng1 states: *"I don't think we do any motivation. We do more of*

ensuring compliance by showing people what they need to know from the organization's policies".

4.2.1 Suggestions to Increase Motivation. The study participants provided several suggestions and recommendations on how to motivate employees to change their behaviour and perceptions towards information security and complying with security policies. Participants reported that these suggestions and recommendations were learned through experience and trial and error of what worked and what did not work during many years managing the ISTA program in their organizations.

CISO2 reported that to motivate people, they tried to communicate the importance of ISTA to protect the organizations from various type of risks: *"We focus on explaining the consequences of not following the organization's policies on the business and various types of risks"*. Understanding the types of risks to the organization information systems helps to motivate employees to attend ISTA to be aware of the organization's policies which will enable them to perform their job in secure manner.

"Awareness teams have always developed material based on a compliance and policy risk culture rather than a true business enablement culture, so there's a real opportunity for us to change the conversation and sit down with the business and say, 'These are the risks. This is how security helps you. How can we properly develop and create content that is consumable for you, supports your teams, and also facilitate better customer experience'" Mng4

Effective communication, building trust, and good relationships motivate employees and makes them actively seek to secure the organization's resources and increases reporting of suspicious activities and security incidents. Mng3 states that this has significant effects on motivating employees to participate in an ISTA program: "*Instead of giving them information at the wrong time, we motivate them to come to us and to enable them to identify when to seek help, and then to be able to come to us and to communicate their needs*". Mng4 agrees stating: "*our job is to enable the business, once our employees understand that, through effective communication and trust building, it'll be easy for us to ask them to be involved in our ISTA activities*".

Engaging employees in ISTA activities such as identifying ISTA program needs, the development of ISTA materials, and the implementation and evaluation of ISTA program is also reported as a motivational strategy. Three participants stated that gaining employees' feedback during ISTA material development is useful as it gives them a sense of ownership. Also, the collection of feedback from employees about their training also enhances their involvement with the ISTA program. Mng3, Mng4 and CISO2 argued the engaging employees in ISTA activities proves to be an effective strategy to motive employees and change their perceptions of information security.

Relating information security to an employee's personal life is another way to motivate. For example, when raising employees' awareness about the organization's policies on the use of social media (Facebook, Twitter …etc.), the organization should ensure that the awareness program makes references to issues like personal and children safety when using social media. Mng3 reports: *"If we are running training on social media, we make sure it's about enabling them to be more secure on their personal social media sites, or talk to their parents or children about secure social media use. We find that making that personally relevant is a really good motivator to get staff to come along and be interested and engaged in the session"*.

4.3 Competing for employees' attention

An unexpected finding from this study was the fact that organizations face a challenge in that employees only have a limited amount of attention that can be devoted to ISTA. As organizations have become more governed by rules and regulations, the amount of training of employees has increased and employees now must be trained about occupational health and safety, sexual harassment, discrimination, privacy etc. This has created a situation where there is competition for employees' attention amongst various organizational functions. CISO2 points out: *"There's competition now within organizations to get the attention of employees and to hold their attention for your security awareness program to be effective. It's very difficult these days. Throughout the year, they go through many training programs. They come back to me and say, 'Do you have any idea how many training sessions go through'"*.

The consequence of such competition between various functions inside the organization for the attention of employees is that it is difficult for employees to focus and remember the information provided in ISTA sessions. CISO1 states: *"There's too much information, information overflow. So, if they [employees] go and come out of our training, they forget immediately everything we taught them. They forget as they have to move on to something else and get ready for more training in two days"*.

4.3.1 **Recommendations to overcome this challenge.** The study participants provided several strategies: First, using multiple delivery methods and being creative and innovative in how the organization delivers their ISTA program. *"You've got to be*

innovative in the way that you reach out to your colleagues, constantly refresh themes to try and get the attention of workforce using things like comic heroes, and quizzes, and giving away gifts and toys to people to try to maintain the interest" Mng3.

Second, increase the effectiveness of the ISTA program by to reducing content and increasing motivation. *"We reduced the content and increased motivational aspects, making us more approachable. That was the most important thing after having realized that with all the competition we've got"* Mng3.

Third, focus on employees who deal with sensitive information and processes. The main target in some organizations is to identify those people and develop an ISTA program that targets them to safeguard the information and processes they deal with in their job. CISO2 states: *"We had to let go of the people that didn't have confidential information. That was biggest thing, I think. To let go of those and really concentrate on those people who dealt with confidential information"*. Mng4 agrees: *"We do a targeted campaign for those people who are dealing with very sensitive or very critical information. We do more frequent, more high-touch awareness training and campaigning with that particular group of stakeholders"*.

Fourth, find the right balance between getting people's attention and overwhelming them with ISTA activities. *"Too much awareness is not good, people are getting confused. We've got to try and get a balance, but you don't want to do it so frequently that people become fatigued. We are vying for their attention like many other parties in the organization. You don't want it to feel like spam and become overwhelming. It's really important that we strike the right balance"* CISO2.

Last, to overcome the problem of employees' limited time and attention is to investigate successful ISTA programs in organizations that have similar risk landscapes. *"What I've been finding when I've talked to other organizations that have had successful awareness campaigns,"* Mng3.

4.4 Measuring the Effectiveness of ISTA

The findings of this study show that organizations recognize the importance of evaluating their ISTA program. Respondents, especially in large organizations, reported that they employ various methods to measure effectiveness of ISTA and to monitor the changes to employee behaviour. These include:

a) Measuring security awareness indications (i.e. the number of reports of security incidents and number of incidents from threats addressed in the ISTA program) *"…more number of calls show that people are understanding risks and they are reporting it"* Mng3.

b) Testing the knowledge of employee pre and post training attendance: *"We perform adhoc testing to check whether a person has understood the policy"* Mng1. The participants stated that understanding the policy involves what a policy statement means and how to apply it.

c) Performing phishing simulations: Organizations may hire consultants to *"send fake spam or phishing email or malware to the organization network. It does not impact it, but tests how employees react. It is just to check the implementation of security training and awareness program in the organization"* Mng4. The aim of such an exercise is *"to check [whether] (1) the organization's system or control detect it or not? (2) what does the users do, click on it or report it? If they are aware of this risk and they have understood [the training] they will not click and report it to helpdesk"* Mng4.

d) Collecting feedback from stakeholders: Employees' feedback is also an important indication of the effectiveness of the program. Therefore, Mng3 stated that they capture qualitative feedback from the stakeholders about the program's materials and delivery methods.

CISO2, Mng3 and Mng4 stated that it is very challenging to accurately measure the effectiveness of their organization's ISTA programs. Mng3 stated that *"It's [ISTA evaluation] arguably the hardest area. We use metrics but these metrics can only provide indication of the success of the ISTA program. At the end of the day we deal with very complex issue human behaviour!"*

Mng3 and Mng4 suggested that organizations should use a combination of effectiveness checking techniques to enable them to some extent measure the effectiveness of their ISTA program. They also added that organizations should investigate and identify the best techniques to evaluate their ISTA program which are suitable to their organizational context. For example, organizations may develop an evaluation survey that focuses on measuring employees' behaviour and knowledge of issues around risks related to the organization industry, or common security incidents. Like organizations tailoring their ISTA program with respect to their ISTA needs, it is also vital to tailor effectiveness checking techniques because techniques that work for one organization may not necessarily work for others.

5. Discussion

The main contribution of this study is to address *the need for empirical evidence in the area* by providing insight into how ISTA activities have been institutionalized, and how well they have been resourced, within organizations. This research has identified that the implementation of ISTA activities in different organizational contexts is approached either formally or in an ad-hoc manner. Further, significant differences between the approaches across key ISTA practices were observed. The findings provide recommendations and suggestions on how to: increase motivational aspects of ISTA, overcome the challenge of competition on employees' attention, and overcome the difficulty of measuring the effectiveness of the ISTA program.

5.1 Towards a formal approach to the Implementation of ISTA activities

The findings of this study revealed the differences between ad-hoc and formal approaches that organizations adopt in the implementation of ISTA activities (Table 2). The findings showed the effect of adopting one of these approaches on the quality of ISTA activities in organizations and therefore on the effectiveness of the ISTA program.

There are two main reasons that organizations adopt a formal or ad-hoc approach for the implementation of ISTA.

First, ISTA programs are implemented to comply with standards and regulatory requirements. Organizations that must comply with standards and regulatory requirements (e.g., ISO\IED 27001) are required to provide ISTA to communicate information security policies. Those organizations that see an ISTA program as a regulatory compliance requirement, rather than a valuable control to increase employees' awareness and prevent insider threats, tend to implement ISTA activities using an ad-hoc approach. This has a detrimental effect on the quality of activities and therefore the effectiveness of the ISTA program. This finding supports [32]'s argument that complying with security standards, does not guarantee the quality of the recommended activities in practice. For example, organizations use CBT to gather statistics of who completed the training and how many times they have done it. This helps to fulfil compliance requirements by showing detail on how many, and how often employees complete training. However, several disadvantages were reported by the respondents such as the lack of human interaction, low motivation, and limited preference and learning style. More importantly, statistics around training completion are not good indications of the employee awareness levels.

Second, variations to the implementation of ISTA can be contributed to the maturity and size of the organization as well as aspects of management support and the availability of resources (including time, budget, and personnel). Respondents from large organizations reported that they formally implement the set of activities where ISTA takes place. Whilst in small organizations, because of a lack of resources, training and awareness activities are dealt with more informally and occasionally may not be done at all. Although the data suggested that small organizations usually adopt an ad-hoc approach and large organizations tend to have a more formal and structured approach, we cannot generalize this and conclude this is the case for all organizations. A small organization that realizes the importance of ISTA, or isn't requirements driven, may invest and dedicate more resources to implement ISTA in a more formal manner. Likewise, a large organisation that is compliance driven may use an ad hoc approach.

In terms of the maturity of an organization, most organizations start by implementing an ISTA program to comply with standards requirements and then move towards improving their program to eventually build a culture of security. The maturity of an organization's ISTA program is influenced by the length of time the organization has implemented ISTA: the longer organization has been conducting ISTA activities, learning from past-experience of what techniques have worked and did not work, the more likely the ISTA program is to be mature. This finding is in line with Manifavas et al. [34] conclusion that "the maturity of the program can play a significant role in its effectiveness; the latter cannot be guaranteed during the first years of deployment" (p.259). Additionally, organizations that have a dedicated team managing ISTA will have more opportunities to improve their ISTA program and to achieve a high maturity level and institutionalized activities. This is because having a dedicated team enables the organization to leverage learning from past-experiences

Identify ISTA program needs is one of the key activities that has been reported by the participants. The findings of this study provide insight on how this practice is conducted in organizations. A formal approach to this activity uses various inputs (security policy, recent risk assessment and incident response reports) to accurately identify the requirements for the ISTA program. However, an ad-hoc approach tends to only use the security policy as an input, which may lead to the organization's needs not being met.

Table 2. Differences between ad-hoc and formal approaches to the implementation of ISTA activities.

ISTA activities	Ad-hoc approach	Formal approach
Identify ISTA Program needs	Only use policy as an input to identify the needs for ISTA	Use various inputs: policy, incident reports, risk assessment, threat intelligence, users' feedback, roles and responsibilities
Develop ISTA program plan	Limited planning activity – only schedule	Thorough planning activities, covering long term (strategic) and short term (tactical) aspects of ISTA
Establishing ISTA program development team	Security manager doing ISTA plus other security responsibilities	Have dedicated team 2 to 3 people (internal awareness manager and external awareness manager)
Develop ISTA materials	Use existing material or PowerPoint sliders	Using various delivery methods that are tailored to the organization's needs. Users are not involved
Conduct ISTA	Only mandatory security training via CBT, occasional awareness massages. Focus on providing knowledge	Have diverse types of ISTA such as intensive awareness campaigns, ISTA for specific for groups and teams as well as the mandatory. Focus on knowledge and motivation.
Evaluating ISTA program	Depend on statistic from CBT	Employ various techniques to measure the effectiveness of ISTA program

The differences between an ad-hoc and a formal approach can also be seen in the *development of an ISTA program plan*. In the formal approach, the ISTA plan is more formalized and extensive, covering both long term (strategic) and short term (tactical) aspects of ISTA. While in an ad-hoc approach, planning covers a few high-level elements such as scheduling of activities.

Organizations that adopt an ad-hoc approach do not have a dedicated team to *manage the ISTA program*. The responsibilities for the ISTA program usually fall to the security manager who is also responsible for other information security practices. Organizations that adopt the formal approach have a dedicated team, one to three people, usually with no technical background (i.e. communication or change management backgrounds) and with a good understanding of the security issues as well as business processes. Having a dedicated team will ensure clear assignment of roles and responsibilities which is important for the success of an ISTA program.

In terms of *conducting the ISTA program*, organizations that implement an ad-hoc approach only use computer based training (CBT), whereas in organizations using a formal approach, several types of ISTA activities will be conducted. The difference in the extent of the implementation of conducting ISTA can be contributed to the lack of resources and the low awareness of the role of ISTA in protecting the organizational information resources in smaller organizations. The literature suggests that to increase the effectiveness of ISTA, organizations should implement the program using various methods, not just CBT [35]. The use of many delivery methods increases the effectiveness of ISTA as it considers the preferences and the learning style of employees in the organization. Subsequently, the selection of delivery methods should take into consideration the type of message and the intended target audience [29].

The findings of this study show that organizations recognize the importance of *evaluating their ISTA program*. The formal approach for ISTA evaluation uses various methods (see Section 4.4) to measure the effectiveness of ISTA and to monitor changes to employee behaviour. However, organizations that adopt an ad-hoc approach depend on training statistics generated by CBT to track the effectiveness of ISTA. This is done mainly to meet compliance and regulatory requirements, not to measure the effectiveness of the program[36]. That means that in these kinds of organizations their ISTA program may not be optimal.

5.2 Developing an effective ISTA program

The study participants provided insights and recommendations on strategies to create an effective ISTA program through focusing on motivating aspects. These recommendations include: motivate employees through effectively communicating the purpose of the ISTA program, building trust and good relationships with stakeholders, engaging stakeholders in managing ISTA activity through providing feedback, and relating the ISTA messages to the employees' private life. The participants also stated that by relating information security to the employees' personal life motivated them about information security. To the best of our knowledge, using personal life to motivate has not been reported in the literature.

Several recommendations were also provided by the participants to overcome the challenge of

competition with other organization training initiatives for employees' attention. First, organizations should consider using multiple delivery methods and try to be creative and innovative in the way the organization delivers their ISTA program. Second, organizations should reduce content and increase motivation. Third, organizations should focus on employees who deal with sensitive information and processes. These recommendations have been reported in the current literature. However, the findings of this study extend the literature by suggesting that organizations should look at consolidating training across organizational functions to reduce the number of training courses and to reduce the competition for employee's attention. For example, the induction training program for new employees should embed basic information security training. This requires constant liaison and communication between HR people and the information security personnel who are responsible for the security awareness and training program. Our suggestion is in line with Puhakainen and Siponen [37] recommendation to integrate the ISTA program with normal business communication of the organization.

The findings of this study show that current techniques and methods employed in organizations to measure effectiveness of ISTA can only provide an indication, but not a comprehensive assessment, of the effectiveness of the ISTA program. For example, the study respondents stated that the number of reports of security incidents around threats addressed in the ISTA program is used as an indication for the level employee's security awareness. However, the number of security incident reports does not necessarily reflect the extent to which the ISTA program is effective in imparting an awareness of risk for two reasons. First, 'incidents' are variably defined and that not every event is an incident. Second, increases in incident reports may occur as a result an increase in the number or sophistication of attacks. Therefore, it is still unknown to organizations how effective their ISTA programs are in changing employee's behaviour and how much they should invest on ISTA to be able to get an effective outcome. This is still an elusive goal for organizations to achieve. The findings suggest that the organizations should use a combination of effectiveness checking techniques enable them to measure the effectiveness of their ISTA program. It is also recommended that organizations develop their own success metrics to measure their ISTA program.

6. Conclusion

This paper has presented an exploratory study of the implementation of ISTA program in six organizations. The study has provided an account of how an ISTA program is implemented in different organizational contexts. It identifies two approaches (ad-hoc and formal) that organizations adopt in the implementation of ISTA activities and discusses the significant impact of each approach on the effectiveness of ISTA in organizations. Further, three challenges have been identified: the lack of motivational aspects in current ISTA program, the competition for employees' attention and the difficulty in measuring the effectiveness of ISTA program. Several recommendations and suggestions were outlined to overcome these challenges.

The findings of the study have several practical implications. They provide guidance on how ISTA activities can be implemented in a more formal and institutionalized approach. The study also provides practitioners with strategies and recommendations to develop an effective ISTA program.

The findings provide a sound basis for further empirical work. The next step is to conduct a set of in depth case studies within organizations which will include several data collection techniques (expert interviews, documents analysis and observation) to gain an in-depth understanding of current ISTA management practices. This will enable researchers to develop a maturity model which organizations can use as an assessment tool to assess their implementation of ISTA and to identify ways to improve their ISTA program.

7. References

[1] Accenture & HfS Research, The State of Cybersecurity and Digital Trust: Identifying Cybersecurity Gaps to Rethink State of the Art, in, 2016.

[2] Crowd Research Partners, Insider Threat Soptlight Report, in, 2017.

[3] P. Balozian, D. Leidner, Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory, SIGMIS Database, 48 (2017) 11-43.

[4] N.N.A. Molok, A. Ahmad, S. Chang, Understanding the factors of information leakage through online social networking to safeguard organizational information, in: Proceedings of the 21st Australasian Conference on Information Systems, 2010.

[5] A. Ahmad, R. Bosua, R. Scheepers, Protecting organizational competitive advantage: A knowledge leakage perspective, Computers & Security, 42 (2014) 27-39.

[6] Australian Cyber Security Centre, 2016 Threat Report, in, 2016.

[7] D. De Maeyer, Setting up an Effective Information Security Awareness Programme, in: ISSE/SECURE 2007 Securing Electronic Business Processes, Vieweg, 2007, pp. 49-58.

[8] SANS, Security awareness report: It's Time to Communicate, in, 2017.

[9] B. Khan, K. Alghathbar, M. Khan, Information Security Awareness Campaign: An Alternate Approach, in: T.-h. Kim, H. Adeli, R. Robles, M. Balitanas (Eds.) Information Security and Assurance, Springer Berlin Heidelberg, 2011, pp. 1-10.

[10] A. Ahmad, S. Maynard, G. Shanks, A case analysis of information systems and security incident responses, International Journal of Information Management, (2015).

[11] P.E. Chaudhry, S. Chaudhry, R. Reese, Developing a model for enterprise Information Systems Security, Economics, Management and Financial Markets, 7 (2012) 587-599.

[12] E. Kritzinger, E. Smith, Information security management: An information security retrieval and awareness model for industry, Computers & Security, 27 (2008) 224-231.

[13] M. Alshaikh, A. Ahmad, S. Maynard, S. Chang, Towards a Taxonomy of Information Security Management Practices in Organisations, in: 25th Australasian Conference on Information Systems, Auckland, New Zealand, 2014.

[14] P. Shedden, A. Ahmad, A. Ruighaver, Organisational learning and incident response: promoting effective learning through the incident response process, (2010).

[15] ISO/IEC, ISO/IEC 27002 Interntional Standard: Information technology - Security Techniques- Code of practice for information security controls, in, 2013.

[16] A. Ahmad, S. Maynard, Teaching information security management: reflections and experiences, Information Management & Computer Security, 22 (2014) 513-536.

[17] M.E. Whitman, H.J. Mattord, Management of information security, 2nd ed., Thomson Course Technology, Boston, Mass., 2008.

[18] M. Wilson, J. Hash, Building an information technology security awareness and training program, in: NIST Special publication, 2003, pp. 50.

[19] G. Öğütçü, Ö.M. Testik, O. Chouseinoglou, Analysis of personal information security behavior and awareness, Computers & Security, 56 (2016) 83-93.

[20] J. D'Arcy, A. Hovav, D. Galletta, User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20 (2009) 79-98.

[21] M. Karjalainen, M. Siponen, Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches, Journal of the Association for Information Systems, 12 (2011) 518-555.

[22] R. Herold, Managing an information security and privacy awareness and training program, CRC press, 2010.

[23] P. Bowen, J. Hash, M. Wilson, SP 800-100. Information Security Handbook: A Guide for Managers, in, 2006.

[24] R. Power, D. Forte, Case Study: a bold new approach to awareness and education, and how it met an ignoble fate, Computer Fraud & Security, 2006 (2006) 7-10.

[25] T.R. Peltier, Implementing an Information Security Awareness Program, EDPACS, 33 (2005) 1-18.

[26] J.A. Valentine, Enhancing the employee security awareness model, Computer Fraud & Security, 2006 (2006) 17-19.

[27] T.R. Peltier, How to build a comprehensive security awareness program, COMPUT SECUR J, 16 (2000) 23-32.

[28] A.C. Johnston, M. Warkentin, Fear appeals and information security behaviors: an empirical study, MIS quarterly, (2010) 549-566.

[29] J. Abawajy, User preference of cyber security awareness delivery methods, Behaviour & Information Technology, 33 (2014) 237-248.

[30] PCI, Information Supplement: Best Practices for Implementing a Security Awareness Program, in, Security Awareness Program Special Interest Group PCI Security Standards Council, 2014.

[31] A. Tsohou, M. Karyda, S. Kokolakis, E. Kiountouzis, Managing the introduction of information security awareness programmes in organisations, European Journal of Information Systems, 24 (2015) 38-58.

[32] M. Siponen, R. Willison, Information security management standards: Problems and solutions, Information & Management, 46 (2009) 267-270.

[33] W.L. Neuman, Social research methods: Qualitative and quantitative approaches, Sixth ed., 2006.

[34] C. Manifavas, K. Fysarakis, K. Rantos, G. Hatzivasilis, DSAPE – Dynamic Security Awareness Program Evaluation, in: T. Tryfonas, I. Askoxylakis (Eds.) Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, 2014, pp. 258-269.

[35] E.B. Kim, Recommendations for information security awareness training for college students, Information Management & Computer Security, 22 (2014) 115-126.

[36] T. Tan, A. Ruighaver, A. Ahmad, Information Security Governance: When Compliance Becomes More Important than Security, in: K. Rannenberg, V. Varadharajan, C. Weber (Eds.) Security and Privacy – Silver Linings in the Cloud, Springer Berlin Heidelberg, 2010, pp. 55-67.

[37] P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, Mis Quarterly, 34 (2010) 757-778.