Investigation of Stakeholders Commitment to Information Security Awareness Programs

Jenal H. Abawajy†, K. Thatcher† and Tai-hoon Kim‡

†School of Engineering and Information Technology, Deakin University, VIC., 3217, Australia.
‡Hannam University, Korea
Science and Engineering Research Support Center
Ojeong-dong Daedeok-gu, Daejeon306-791, Korea

Abstract
Organisations have become increasingly dependent on technology in order to compete in their respective markets. As IT technology advances at a rapid pace, so does its complexity, giving rise to new IT security vulnerabilities and methods of attack. Even though the human factors have been recognized to have a crucial role in information security management, the effects of weakness of will and lack of commitment on the stakeholders (i.e., employers and employees) parts has never been factored into the design and delivery of awareness programs. To this end, this paper investigates the impacts of the availability of awareness programs and end-user drive and lack of commitment to information security awareness program design, delivery and success.

Keywords: Human factor, Security, IT security, security awareness training

1. Introduction
With the increasing penetration of information technology into everyday life, the knowledge of IT systems and its potential for misuse has exploded. Moreover, the rate at which the risks to information security have increased is much greater than that of the ways to counter these risks [3]. Also, there has been widespread awareness of the security risks to information technology and the need for methods to combat these risks.

In general, there is a tendency for organizations to adopt technology-based remedial measures such as authentication and firewall systems to minimise potential risks to information technology [6]. However, in spite of heavy investments in strong security perimeters, companies and corporations all over the world continued to lose billions of dollars in business transactions and valuable assets [3]. This suggests that not only does the organisation need to worry about threats from the outside, such as hackers, but they should also be worried about the measures that employees are not taking on a day-to-day basis [7]. Therefore, human factors such as user awareness and operator carelessness are as important as technical factors such as encryption and firewall systems. An intuitive approach to address security risks due to human factors is by making appropriate security awareness programs available to employees that directly or indirectly deal with the information technology.

Given this identified problem space, the overall research question of this paper is to explore how human factor related information security considerations can be integrated into the overall enterprise information system. The quest to solve this problem is divided into three research questions as follows:

1. How often do organizations provide information security related training programs to employees?
2. Is their a desire on the part of employees to be knowledgeable in information security related issues of their workplace?
3. How often employees take the initiatives to gain IT security related training programs on their own?

The aim of the first research question is to investigate the level of understanding and the importance of information & IT security within the organisation while remaining cognisant of the different risk environment created by employees. This question is important as corporate stakeholders have increasingly pressed executives for accountability in all endeavors, including security training grows [15]. It is also imperative that the employees take upon them to keep abreast with the various attack techniques and available tools to combat them. In exiting studies, the
effects of weakness of will and lack of commitment on the employee parts are not taken into account. The aim of both the second and the third research questions is to fill this void.

The main contribution of this paper to the knowledge base on information security is that how the human factor specifically the stakeholders drive and lack of commitment to information security training impacts the security culture and subsequent security awareness program design and delivery impacts. Using survey-based approach to understand what people’s attitudes and awareness towards information security are and how people different age groups have different knowledge and attitudes towards it. The findings of the survey will help understand what people’s attitudes and awareness towards information security are and how people different age groups have different knowledge and attitudes towards it. This knowledge will help identify the main areas in which different age groups have varying level of education and their knowledge in areas such as information security.

The rest of the paper is organized as follows. In Section 2, we discuss the background and place the research questions within the context of exiting research frameworks. It also discusses the different areas that relate to security awareness and how education and work environments contribute the way an employee conducts themselves in regards to computer security. In Section 3, the results of the empirical research are presented. We discuss the results in Section 4. The conclusion is presented in Section 4.

2. Background and Related Work

These days, most businesses depend heavily on information technology and their disruption for even a few days could cause severe financial as well as reputation loss and threaten survival. Due to the expanded use of the Internet by institutions, business organizations and individuals on the one hand and by criminals and abusers on the other hand, the importance of information security has recently increased globally.

The ongoing attacks such as viruses and hacking have prompted organizations to ensure that appropriate security defences exist within their organisation [3]. An attack is a deliberate act that exploits vulnerabilities and could be generally classified as technical and non-technical. Technical attacks such as IP spoofing and denial of service often exploit security design flaws (e.g., implementation flaws and inadequate protection features). In contrast, non-technical attacks such as social engineering exploit behavior of individuals interacting with systems (e.g., poor usage practices, inexperienced or inadequately trained users, incorrectly disposed of documents).

On technological front, the IT security industry has made significant advances with a huge number of technical protection solutions in the areas of computer and communications security to meet the perceived threats to business organizations. The perimeter security models have become a common practice for protecting critical business infrastructures and information. In particular, security controls between the Internet and an organization’s internal network have become a consistent focus of technology spending. Although these organizations may have established strong perimeter security, it represents only a first line of defence. Therefore, when it comes to information technology security, there is more than just the technical aspect [8, 9].

In particular, from the information system user’s point of view only limited solutions have been presented. Having a strong security perimeter using tools such as authentication and firewall systems only serves to lure the organizations into a false sense of security. The real security is the security from within the organisation, involving its employees, processes and workflows. For examples, employees tend to be the weakest link in the security chain [9] and the major threat to IT infrastructures is constituted by careless employees who do not comply with organisations security policy and procedures [10]. The key threat to information security is from careless employees who do not comply with information security policies [10]. Therefore, human factors such as lack of awareness and lack of adherence to usage policies can cause loopholes in systems that have been secured in technical aspects [8]. By not understanding the potential risks to the organisation, by not recognising potential threats when they see them, or by careless actions, employees could render any secure system into insecure system [9].

Punishment could be used to minimizing user-related faults in information security. However, scholars of the behavioural community have presented much evidence of the negative long-run consequences related to the use of punishment, for instance loss of productivity, increased dissatisfaction, and aggression [13]. An alternative approach is for the employees working in the information technology to be aware of the security issues that could be faced the organization on a day-to-day basis [7]. To address this problem, the availability of constant training and awareness’s programs in information security to employees is paramount.

Security training and education offers employees at all level in the workplace the appropriate behaviours and best security practices they need to help their
organisations reduce IT risks. The importance of awareness has been underlined since it has been perceived instrumental to the effort of reducing 'human error' [14]. The topic has been approached systematically, and a conceptual foundation for organizational information security awareness that differentiates between the framework (‘hard’, structural) and content (informal, interdisciplinary) aspects have been developed [7]. Al-Hamdani [12] suggests that “the purposes of awareness presentations are simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly”. There are many tools which can be used to inform the employees about information security. “A few examples of IT information security awareness materials/activities include promotional speciality trinkets with motivational slogans; a security reminder banner on computer screens, which comes up when a user logs on; information security awareness videotapes; and posters or fliers” [12]. Many organisations adapt these measures, as most of them are inexpensive to produce in bulk and distribute across a large organisation. However, in all the models, the impact of the stakeholders (i.e., employers and employees) drive and lack of commitment to information security training and subsequent security awareness program design and delivery have largely been ignored.

Unlike existing research, we believe that creating a culture of security is an essential corporate governance initiative for any organisation. Moreover, existing research is based on implicit assumption that the end-user of information technology do want to take part in the awareness programs. We believe that both the employer and employees have the responsibility to ensure the security of the information technology and thus have the responsibility to engage in the security awareness and training programs. The employers have vested interests to make the training programs available to its employees on regular bases. Similarly, the employees have the responsibility to keep abreast with the security risks facing the information technology, the techniques used by hackers as well as the available tools to combat the threats. The question we address in this paper is how often that both the employees and the employers play their respective roles in making sure that information technology assets are well secured?

The main contribution of this paper to the knowledge base on information security is that how both employees and employers attitude and awareness towards information security. Using survey, we investigated the availability of security-related training programs for information technology users within the workplaces. This is very important as educating information technology users on the importance of security is vital to the mission of any organisation [11]. The participants were questioned about the IT security training program within their organisation, if they have been given any training and if not to see if they are interested in being trained in the security of the IT within their workplace. The results of the survey is then extrapolated and analysed. Web based questionnaires were chosen for this study as it has the ability to reach a number of people at the one time. They allow for the identity of the participant to remain anonymous and allow for the data to be immediately stored after the completion of the questionnaire. The web based questionnaire that has been created to collect data for this study is compatible with the mainstream web browsers. This means that the participants should not have a problem viewing or completing the questionnaire. They layout of the questionnaire is the standard layout that is applied by the online questionnaire tool. The placing of the different sections and order of the questions were considered by the researcher rather than the actual layout of the questionnaire.

3. Survey Results

We asked the participants, if there organisation holds information security trainings to employees (e.g., courses, workshops, and seminars). In response, 39.39% of participants said that their organisations do hold information security training, whilst 60.61% said that their organisations did not hold any information security trainings.

<table>
<thead>
<tr>
<th>Questions</th>
<th>YES (%)</th>
<th>NO (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your organisation hold courses/workshops/seminars that focus on organisation security?</td>
<td>39.39%</td>
<td>60.61%</td>
</tr>
<tr>
<td>Have you attended any courses/workshops/seminars, which have focused on IT Security?</td>
<td>43.75%</td>
<td>56.25%</td>
</tr>
<tr>
<td>Would you be interested in completing an IT Security course/workshop/seminar?</td>
<td>33.33%</td>
<td>66.67%</td>
</tr>
</tbody>
</table>

Table 1: Results of the survey.
security but their organisation did not hold any such events, and 18.75% of participants said that they had not attended any courses/workshops/seminars that focused on organisation security but their organisation did hold sessions such as this. 37.5% of participants said that they had not attended any courses/workshops/seminars that focused on organisation security and their organisation also did not hold such events.

In response to the question: Have you attended any courses/workshops/seminars, which have focused on IT Security? The result shows that just under half of participants that completed the study had some prior knowledge of IT security. 43.75% of participants had attended some sort of course/workshop/seminar, which focused on IT Security, whilst 56.25% of participants had not attended any courses/workshops/seminars that focused on IT Security.

We then asked if those participants who answered ‘NO’ to the previous question, if they would be interested in completing an IT Security course/workshop/seminar. 33.33% of participants said that they would be interested in completing an Information Technology Security course/workshop/seminar in the future, whilst 66.67% said they had no interest in completing such a course/workshop/seminar. This shows that only one third of the participants that completed this question had some interest in computer security. Most employees will perform these tasks if there is a strong culture within the organisation that holds security as an important matter.

4. Discussion

As the number and successes of attacks have increased, information security has become increasingly important for majority of organizations [3]. The main principle of information security is to sustain and support the mission and operation of an organisation [1]. Information security awareness program is the key elements of an information security. Organisations have become increasingly dependent on technology in order to compete in their respective markets. As IT technology advances at a rapid pace, so does its complexity, giving rise to new IT security vulnerabilities and methods of attack. An organisation’s IT security system must match this acceleration in order to contend with anything/anyone that could harm its operations and/or functionality [5].

There are enough evidences that improved employee understanding of appropriate behaviours and best practices for enhanced information security reduce security risks. Employees are generally not aware of the security measures that they can take on a day-to-day basis to help prevent security breaches. Simple tasks such as keeping passwords secret and locking their computer screen when they leave their computer can be effective in preventing unauthorised personnel from accessing the organisation’s information. Most employees will perform these tasks if there is a strong culture within the organisation that holds security as an important matter.

Given the environment of government oversight and regulation, and the adoption of new information technology, enterprise training to improve information security is likely to remain a high priority. However, a recent survey of over 400 IT managers show that support for security training fell to below 50% for the first time, as most managers believe that it is ineffective [16]. This means that merely providing security training is not enough. Organisations need to know if training programs have been successful in changing employee behaviour. Organisations need to know if training programs have been successful in changing behaviour. This requires metrics that help establish a baseline of individual and organisational competencies in enterprise security be set in place from the start. Perhaps the most employed method to evaluate learning achievement is the Kirpatrick method [17]. Kirkpatrick’s four-level learning model (reaction, learning, behavior and results) is the most widely used and accepted method for measuring learning effectiveness today. By employing Kirpatrick’s education model and the security industry best practices, organisations can successfully assess the effectiveness of its security awareness training program, measure the results, and further improve the training.

When it comes to information technology security, there is more than just the technical aspect [8, 9]. The education of employees in relation to security generally falls on the IT managers and this is where information security awareness programs become an important part of an organisation’s procedures. Siponen argues that with regard to security guidelines, education should aim at the users internalizing the needs that drive the security guidelines [10]. Thus, it is important that security guidelines are justified as normative claims, i.e., arguments and justifications are given. As a result, users may change their attitude and motivation towards the guidelines in the intended way, and attain prescriptive awareness of the subject of security, which is central target of the awareness approach. These are few methods in which awareness within an organisation can be enhanced by managers taking an active stand on security issues. For example, IT staffers can maintain awareness by providing their user community with regular updates on technology threats and security issues. Moreover, IT managers interested
in fostering security awareness will often dedicate specific sections of regular status reports to security. Such a security section should incorporate the system status; identify weaknesses or risks, and reference activities or resources that could mitigate the risk”.

5. Conclusions and Future Direction

Research shows that security breach, in many cases, originates from inside the organisation rather than from outside the organisation. For an organization to effectively safeguard critical information, it takes more than integrating the latest security hardware and software. This research finds that security awareness programs must be seen by top management and security professionals as an effective medium in which to communicate the organisation's security policy and other important security information to the employees. To the best of our knowledge, there is no study that prompts whether or not the organisations make security-related training programs available to its employees on regular bases. Similarly, there are no studies that look at the case if individuals themselves take the initiatives on their own and at their time and cost to keep abreast with the security risks to information technology and available tools to combat them. Our research shows that the effects of weaknesses of will and lack of commitment on the employee parts must be taken into account in the design and delivery of awareness programs.

Acknowledgement: This paper would not have been possible without the help of Maliha Omar.

6. References


[16]. Iain Thomson, Security no longer top IT concern, Personal Computer World, 30 Jan 2008