Significance of Information Security Awareness in the Higher Education Sector

Hong Chan
School of Medicine, Discipline of Medicine
University of Adelaide, Australia

Sameera Mubarak
School of Computer and Information Science,
University of South Australia, Australia

ABSTRACT

Information security awareness is an important contributing factor for a successful information security plan and should be properly assessed in order to suggest improvements. This explorative study directly investigated and assessed the employee information security awareness levels within a South Australian Higher Education Institution for the purpose of providing much needed insight into the extent of information awareness levels in Australian organizations. Using an online questionnaire, the study revealed that the organization's employee information security awareness were generally lacking. The study also identified several problem areas which had plenty of room for improvements, thus paving the way for further research into how information security awareness levels can be improved. It is recommended that the organization include information security awareness as part of its overall risk assessment strategies in order to mitigate such risks. Finally, the adoption of programs which will enhance security awareness should also be explored in order to foster an organizational culture of security compliance, thereby minimizing any information security risks.

Keywords

Information Security, Information Security Awareness, Information Assurance, Information Management.

1. INTRODUCTION

Due to advances in information technology and the resultant high accessibility of information by internal and external users, information security has become highly relevant and necessary for the survival of organizations [1,2,3]. Failure to protect confidential information may result in exorbitant costs in public liabilities, which may result in the ultimate downfall of an organization.

There are three important aspects of information security according to Cervone [2]. Firstly, the confidentiality aspect relates to preventing unauthorized access to information, thus ensuring that confidential data or information is well protected. Secondly, integrity relates to the accuracy, correctness and currency of information, thus ensuring that information is trustworthy and faithfully represents the real world in which the data or information is based on. Thirdly, availability of information relates to ensuring that authorized access to information or systems are provided when needed.

The main purpose of information security, therefore, is to ensure business continuity in order to minimize damage and liability to the organization. Furthermore, organizations have both an ethical and legal responsibility in ensuring that confidential information is well protected [2].

Many papers such as von Solms [1] and Cervone [2] have concluded that to counteract or to minimize the risk of information security breaches, it is important for an organization to implement an information security plan or strategy.

Further, Namjoo et al. [4] suggested that the preventative actions by organizations usually take place after the occurrence of information security breaches. By the time an incident has taken place, it could be too late. It is therefore better to be safe than sorry.

Information security measures usually consist of utilizing technical controls in order to mitigate information security risks. However, Dzazali, Sulaiman & Zolait [5] stated that technical controls become futile if the people interacting with the information systems do not have prudent security practices. In other words, human factors must be taken into account. Policies or controls become useless if users are not aware of any security risks or the policies themselves.

It is widely accepted within current literature that information security awareness is a key factor in contributing to a successful security strategy [4,6,7,8,9,10,11,12,13]. Further, there is a positive and direct relation between information security awareness and preventative action and thus improved security performance [9] which suggests that employee security awareness assessment should be the starting point in developing or enhancing any security strategies.

According to Bulgurcu, Cavusoglu & Benbasat [13], information security awareness is an employee's knowledge of information security concepts and his or her consciousness of the organization's information security measures or plans.

Due to the apparent gap which exists in current literature in that studies in relation to organizational information security awareness in an Australian context are minimal, this investigative study aims to assess the employee awareness levels of an Australian organization. Assessment was conducted using a questionnaire in which the design and methodologies were based on the study presented by Kruger, Drevin & Steyn [14]. The questionnaire was delivered online and the resultant collected data was analyzed to gain insight into employee awareness levels.

2. BACKGROUND

The following sections provide a review of current literature relating to information security awareness and within the scope of this study.

2.1 Need for Information Strategy

Bulgurcu, Cavusoglu & Benbasat [13] defined information security awareness as an employee's knowledge of information security and his or her consciousness of the organization's information security measures or plans. Bulgurcu, Cavusoglu & Benbasat [13] investigated employee rationality based behaviors, information security awareness, and their effects on information security compliance. The study was able to show that an employee's intention to comply is greatly influenced by their attitude and their outcome beliefs. More importantly for the purpose of this research, the study found that an employee's attitude and outcome beliefs are affected by their level of information security awareness. In other words, placing emphasis on information security awareness can positively affect employee attitudes and to encourage compliance.

Spears & Barki [7] explored the relationship between employee participation in risk management and internal security compliance. The study was able to conclude that employee participation in risk management greatly contributed to improved security control performance due to greater alignment between security risk management and the business environment, better policy development, and more importantly for the purpose of this research – greater information security awareness. While the study did not explore information security awareness as the main driver of a successful security policy, it did highlight information security awareness as a main contributor.

2.2 Managerial Contributions to ISA

It is important to examine existing literature on managerial information security awareness. McFadzean, Ezingeard & Birchall [8] identified the awareness of senior management as an important driver of effective security measures. The study argued that senior executives have a holistic view of the organization and therefore have the power to affect change in the organization through their roles as strategy implementers. It was found that board level perceptions and thereby information security awareness are positively related to the strategic activities of an organization.

Similar to McFadzean, Ezingeard & Birchall [8], Knapp et al. [9] also identified senior management as key players. The study found that senior management support is positively related to both an organization's security culture and the level of policy enforcement. While the study did not directly explore managerial information security awareness as a predictor of security performance, it did again highlight the importance of management involvement, thus the importance of managerial information security awareness in affecting an organization's information security readiness.

Mouratidis, Jahankhani & Nkhoma [10] aimed to study the differences in perception of network security between general management personnel and personnel who are responsible for actual network security. The study found that general managers do have different perspectives towards network security than personnel from the network security management. In particular, the effectiveness and efficiency of networks, control of security, security decision making process, and users of the network all showed significant perceptual differences. There is a clear lack of information security awareness within general management and as confirmed by McFadzean, Ezingeard & Birchall [8], this could have a negative impact on the effectiveness of information security policies.

Namjoo et al. [4] further reinforced the importance of information security awareness levels of management by investigating the relationship between managerial information security awareness and action. The study was able to provide empirical support for a positive relationship between awareness and action. In other words, the higher the level of managerial information security awareness, the more likely the managers will take action in implementing preventative measures. The study suggested that preventative action usually occur after the fact. That is, unless an actual information security breach has occurred, organizations usually take no action in adopting security measures. Like various similar studies, Namjoo et al. [4] implied that by raising managerial information security awareness, information security performance could in fact improve information security performance.

2.3 Australian ISA – National Perspective

The exploratory study conducted by Lane [15] identified that in relation to information security management in Australian Universities, information security awareness activities remain a challenge. The study suggested that Australian Universities do not have adequate security awareness programs in place to counteract the low levels of awareness, therefore compliance is also low. Thus it is important to adapt information security awareness programs in order to foster a culture of compliance, which will ultimately enhance employee compliance of information security.

In another Australian Higher Education context, and similar to Spears & Barki [7], Yeo, Rahim & Miri [16] explored security risk assessment strategies of an Australian University. Again, the study only briefly discussed the implications of user's information security awareness. The study identified security awareness as an important component which must be assessed as part an organization's risk assessment. User non-compliance is a serious risk for any organizations, and awareness is positively related to compliance. The study concluded that information security awareness of employees must be risked assessed as part of an overall organizational risk assessment strategies in order to identify areas which need improvements. In other words, the lack of information security awareness poses serious threats to an organization and must be properly risk assessed and mitigated.

2.4 International Perspective on ISA

Hagen, Albrechtsen & Hovden [11] studied the implementation of organizational security measures and to assess the effectiveness of such measures. It was discovered that many Norwegian organizations placed emphasis on the policies and procedures in implementing any measures, but placed very little emphasis on security awareness. The study also showed that awareness measures were the most effective of any security measures. As a consequence, the study showed an inverse relationship between the implementation of security measures and their effectiveness. In other words, it is important to place emphasis on security awareness as well as technical controls when adopting security programs. Hagen, Albrechtsen & Hovden [11] only investigated Norwegian organizations. However, due to the similar structures of western organizations (similar accounting practices, management hierarchies, information technology infrastructure etc.), it can be posited that Australian organizations are in a similar situation.

In recent years, ensuring the security of information has become extremely complex and challenging. This is more so for Universities because teaching and research activities are becoming more reliant on the availability, integrity and accuracy of computer based information [12]. The study conducted by Doherty, Anastasakis & Fulford [12] aimed to empirically study the structure or content of security policies for UK based Universities in order to fill the gap in the literature by critically examining the structure and content of these policies. The study found that due to the wide diversity of these policies, it was not possible to foster a coherent approach to security management. It also found that the range of issues being covered in such policies was surprisingly low, and reflects a highly techno-centric view rather than a user-centric view of information security management. This suggests that the user or staff information security awareness are not prominent nor considered in these policies. Again, while Doherty, Anastasakis & Fulford [12] only explored UK based Universities, it can be posited that Australian higher education institutions such as the subject of this study may have similar attitudes, thereby further justifying the need to explore information security awareness in an Australian setting.

Laaksonen & Niemimaa [17] conducted an exploratory study into information security policies and their effectiveness. However, the study did suggest that information security awareness did influence employee perception of security policies and therefore must be taken into account when devising such policies.

2.5 Assessing ISA

In determining a positive relationship between information security awareness, employee rationality based behaviors and policy compliance, Bulgurcu, Cavusoglu & Benbasat [13] included three simple questions in their questionnaire to gauge security awareness. These questions are:

1. I know the rules and regulations prescribed by the ISP of my organization.

2. I understand the rules and regulations prescribed by the ISP of my organization.

3. I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.

As can be seen, these questions are all directly related to an organization's existing information security policy (ISP as stated in the questions) and do not involve gauging an employee's awareness of information security concepts such as social engineering [2]. While there are clear limitations to the methodology of Bulgurcu, Cavusoglu & Benbasat [13], the study did provide a part example of how awareness can be gauged.

Similarly, the study by Namjoo et al. [4] looked at information security awareness of managers in determining its relationship and managerial action relating to prevention. Like Bulgurcu, Cavusoglu & Benbasat [13], simple questions were used to gauge awareness. The questions were again limited in that they were only relevant in the context of an existing security policy.

Perhaps the most extensive tool for assessing information security awareness was proposed by Kruger, Drevin & Steyn [14]. Like many studies, Kruger, Drevin & Steyn [14] acknowledged that an organization's survival necessitates a security program. Due to the importance of information security awareness in ensuring a successful plan, the study proposed that the starting point in developing a plan is to assess awareness levels of employees. The study aimed to examine the feasibility of an information security awareness test for employees, thereby identifying suitable topics to include in an information security awareness training program. It was found that the use of a vocabulary test to assess awareness levels is beneficial in gauging the awareness of employees. It is important to note however, that the test population used by the study were all University students rather than employees from an actual organization. However, for the purpose of this proposed research, the vocabulary test proposed by Kruger, Drevin & Steyn [14] will be modified to fit the Australian organizational context and will be used to assess awareness levels of employees in the organization in question. This will be further discussed in the methodology of the paper.

In summary, all studies reviewed above have identified information security as a key contributor to successful security plans or measures. There is a clear gap in the reviewed literature in that very little studies into information security awareness have been conducted for Australian organizations. As a matter of fact, during the search for literature in relation to this study, only a small amount of studies was found to be related to Australian organizations. More importantly, very little amount of studies have been identified in relation to information security awareness. This further justifies the need for this type of study. The result of this study may provide an insight into the awareness levels, and thus the information security readiness of Australian organizations. Further, it would provide a means to gauge awareness and thus identify any aspects of information awareness requiring improvements to be included in a security training program or security policy.

3. METHODOLOGY

The following sections will discuss the methodologies adopted for the purpose of this study body.

3.1 Aim

The aim of this study is to gain an insight into the information security awareness levels of a South Australian Higher Education Institution's employees in order to identify areas that need improvement. In other words, this study is an investigative or explorative study.

3.2 Research Methods

The nature of this research is exploratory rather than to test for hypothesis. According to Ryerson, cited in De Haes & Van Grembergen [18], exploratory research includes a mixture of secondary research methods such as summarizing quantitative data obtained by surveys and literature review. Therefore, the use of quantitative methods and literature review discussed in section 2 in order to gain insight into the topic of information security awareness was adopted for this study.

3.3 Questionnaire Justification

A questionnaire was used for this explorative study because a related study has proven the use of such questionnaires in assessing information awareness to be both beneficial and practical [14]. The design of the questionnaire was also based on the study conducted by Kruger, Drevin & Steyn [14].

An online questionnaire consisting of five sections and totaling seventeen questions was developed to assess the awareness levels and the behaviors of the employees in relation to various aspects of information security. The web-based deployment of the questionnaire ensures a greater reach and better response rates. The questionnaire requires about ten minutes of the respondent's time for completion and the resulting collected data is immediately available.

3.4 Questionnaire Design

Based on the definition of information security awareness by Bulgurcu, Cavusoglu & Benbasat [13], the questionnaire included two areas to test the respondents' knowledge of common information security concepts and a latter section which gauges an employee's consciousness or awareness of the organization's security and password policies' existence. In addition, employee behaviors in relation to information security were also tested in a third section. The remainder of the questionnaire aimed to obtain the respondent's demographic attribute and an open-ended section which aims to identify any respondent's previous experiences relating to information security incidents or breaches. The ensuing sections will provide an overview of the questionnaire design and the questionnaire can be found in Appendix A.

3.4.1 Section 1 – Knowledge of Concepts

Similar to Kruger, Drevin & Steyn [14], various generally known or common concepts identified in the literature review were included in this section of the questionnaire because the purpose of this study is to explore and to gauge awareness levels of all employee types and not just information security professionals. The underlying assumption is that most general employees would not know the meaning of lesser known concepts such as "botnets" or "Steganography" [14]. All concepts included in this area were identified to be relevant for this study and applicable for the organization in question. A total of five questions are included to assess the respondents' knowledge in the following concepts:

Question 1: Phishing

Question 2: Spam

Question 3: Social Engineering

Question 4: Strong Passwords

Question 5: Information Integrity

The questions are multiple-choice based, with only one possible correct response for each question. The exception to this is question 4: strong passwords in which the question is open-ended in order to prevent respondents from easily selecting the most likely and obvious choice. The choices for the other questions are not so clear or obvious.

3.4.2 Section 2 – Employee Behaviors and Actions

The second section of the questionnaire consisted of scenario based questions. The idea that behaviors should be assessed along with concepts is adapted from Kruger, Drevin & Steyn [14] who observed that there are significant relationships between security concepts and behaviors. The questions in this section evaluate the respondent's action taken in their past based on scenarios within an information security context. The basis for these questions is that the questions are linked with a corresponding security concept being assessed in section 1 of the questionnaire.

No linkages between social engineering and a corresponding behavioral question were identified.

3.4.3 Section 3 – Consciousness of Policies

This section of the questionnaire relates to the second part of the definition of information security awareness as defined by Bulgurcu, Cavusoglu & Benbasat [13]. That is, in addition to the knowledge of concepts, information security awareness also consists of an employee's consciousness or knowledge of an organization's policies in relation to information security. Note that for the purpose of this study, the existence or the details of any organizational policies in relation to information security are not discussed because such information is deemed to be private and confidential. The section consists of two multiple choice questions with each having only one possible correct answer. The first question relates to information security policy and the latter question relates to password policy.

3.4.4 Section 4 – Experiences relating to computer crime

This section of the questionnaire attempts to identify any previous employee experiences relating to security incidents/breaches or computer crime. The purpose is to gain an overview or insights into employee perceptions of such incidents and the actions taken as a result of such incidents. Section 4 consists of three questions. The first question asks whether or not the respondent has ever experienced computer crime. Based on the response, the subsequent questions are open-ended and request details of the experience.

3.4.5 Section 5 – Demographics

The last section of the questionnaire has only one question and simply identifies each respondent's demographic groups. The categories listed in the question's multiple choices will be further combined into two broad categories of management and general employees. The reason for the merging of the categories is that the literature review has identified both management and general employees as distinct groups of stakeholders in regards to information security.

3.5 Data Collection

The online questionnaire was created and deployed using the web-based survey service provider Qualtrics was selected for the task because it is highly secure and can handle the storage of large amounts of responses. The responses can be exported into most commonly used statistical formats such as Microsoft Excel compatible files. Qualtrics also allows for all question types such as multiple-choice, text boxes, and has support for selectively releasing questions based on responses from previous questions. Qualtrics is widely used by many research institutions.

The link to the online questionnaire was distributed to all employees via the internal email system. The email invited all employees to voluntarily take part in the research. Further, the invitation stated clearly that the responses to the survey will remain strictly anonymous and that no individuals can possibly be identified in the collected data. The purpose and details of the research was outlined in the email. The email also stated that by submitting the responses to the online questionnaire, consent was thereby simultaneously given by the respondents.

3.6 Data Analysis

Quantitative methods and Microsoft Excel 2010 were used to obtain tabulated percentages of all responses to closed questions. In addition, content analysis was performed on responses to open-ended questions in order to determine whether the responses were deemed positive or negative. For example, in relation to strong passwords, content analysis was used to group responses into either yes (has knowledge of strong password) or no. Content analysis was performed for open-ended questions which only served to obtain a general overview or insight into the employee perception and actions taken in relation to computer crime or information security incidents. Finally, the cross-tabulation (pivot tables) functionality within Microsoft Excel 2010 was used to show the relationships between information concepts and related behaviors

In summary, the explorative nature of this study justifies the combined methods of data collection via an online questionnaire and literature review (refer to section 2). The use of an online questionnaire ensures a higher rate of responses compared with traditional paper based surveys due to its convenience for respondents. The design of the questionnaire itself is based on principles used in similar studies which have proven to be both practical and beneficial. The results of the questionnaire will be presented in the ensuing section 4.

4. Results

The online questionnaire was distributed to all employees of the organization in question. There are approximately 2400 employees, equating to a population of 2400 for statistical purposes. 308 responses were received in total, representing the sample population of 308. In other words, 12.8% of the organization responded to the questionnaire.

4.1 Demographics

Respondents for this study were managers, general administrative and academic staff.

4.2 Employee's Knowledge of Concepts

Table 1 summarizes the results of the knowledge based questions for each concept as a number of responses and as a percentage of all respondents.

In relation to the concept of strong passwords, respondents were asked to state what they think a strong password should be. Based on manual content analysis, the responses were compared against the definition provided by Microsoft Safety & Security Centre [19] to determine whether the respondent had a good idea of a strong password. For example:

"A mixture of alpha and numeric" was deemed insufficient and therefore deemed incorrect.

"One that uses letters, numbers, and symbols, and has sufficient length" was deemed to be correct.

The criterion for a correct response is that sufficient length, the combination of alpha-numeric, and symbols must all be mentioned.

Table 1. Knowledge of Concepts – All Staff

Concept	Knew the Concept	Responses	Percentage
Phishing	Yes No	76 232	24.7% 75.3%
Spam	Yes No	263 45	85.4% 14.6%
Social Engineering	Yes No	55 253	17.9% 82.1%
Strong Password	Yes No	203 105	65.9% 34.1%
Information Integrity	Yes No	281 27	91.2% 8.8%

Only 24.7% of respondents knew the term phishing. 85.4% of respondents knew what spam is. Only 17.9% of respondents knew the term social engineering. 65.9% of respondents had an idea of what a strong password should be. 91.2% of respondents knew the importance of information integrity.

4.3 Employee Behaviors

Table 2 presents and summarizes the results of section 2 of the questionnaire.

Table 2. Employee Behaviors

Action	Performed Action	Responses	%
Given away passwords or logged someone on using own password	Yes No	163 145	52.9% 47.1%
Left computer unattended and unlocked	Yes No	238 70	77.3% 22.7%
Used inappropriate methods for storing passwords	Yes No	105 203	34.1% 65.9%
Clicked on unknown links embedded in third party emails	Yes No	228 80	74.0% 26.0%
Amended data without confirming accuracy or authenticity	Yes No	24 284	7.8% 92.2%
Disclosed work related information on social networking sites	Yes No	23 285	7.5% 92.5%

A surprising 52.9% of respondents have given away passwords or logged someone onto a computer using their own password. A surprising 77.3% of respondents have left their computer unattended and unlocked. 34.1% of respondents used inappropriate methods for storing passwords. A surprising 74% of respondents have clicked on unknown links embedded in third party emails. Only 7.8% of respondents have amended data without confirming accuracy or authenticity. Only 7.5% of respondents have disclosed work related information on social media.

4.4 Relationships between Concepts and Behaviors

The results of section 4.2 and 4.3 were cross tabulated to gain an insight into the relationship between concepts and corresponding behaviors.

Table 3. Relationships between concepts and behaviors

All Staff		Has clicked on unknown embedded links from third party emails	
		Yes	No
Knew what phishing is	Responses Percentage	172 74.1%	60 25.9%
Did not know what phishing is	Responses Percentage	56 73.7%	20 26.3%
Knew what spam is	Responses Percentage	198 75.3%	65 24.7%
Did not know what spam is	Responses Percentage	30 66.7%	15 33.3%

Surprisingly, 74.1% of respondents who knew the meaning of phishing still clicked on unknown embedded links. Similarly, 75.3% of respondents who knew the meaning of spam still clicked on unknown embedded links.

Table 4. Knowledge of strong password VS behaviors

All Staff		Knew the concept of a strong password			
		Yes		No	
		Response	%	Response	%
Has given away passwords or logged someone in using own password	**Yes** **No**	105 98	51.7 48.3	58 47	55.2 44.8
Has left computer unattended and unlocked	**Yes** **No**	161 42	79.3 20.7	77 28	73.3 26.7
Has used inappropriate methods for storing passwords	**Yes** **No**	61 142	30 70	44 61	41.9 58.1

51.7% of respondents who knew the concept of a strong password have admitted to giving away their passwords. 79.3% of respondents who knew the concept of a strong password have admitted to leaving their computers unattended and unlocked. 30% of respondents who knew the concept of a strong password used inappropriate methods for storing passwords.

Table 5. Knowledge of Information Integrity VS behaviors

All Staff		Has amended data without confirmation or due process	
		Yes	No
Knew the importance of information integrity	Responses Percentage	21 7.5%	260 92.5%
Did not know the importance of information integrity	Responses Percentage	3 11.1%	24 88.9%

7.5% of respondents who understood the importance of information integrity have amended data without confirmation or due process.

4.5 Consciousness of Policies

This section presents and summarizes the results of section 3 of the questionnaire which assesses the awareness or consciousness of existing security policies of respondents.

Table 6. Consciousness of Policies

General Staff	Aware of Policy's Existence	Responses	%
Information Security Policy	**Yes**	**126**	**40.9**
	No	**182**	**59.1**
Password Policy	**Yes**	**101**	**32.8**
	No	**207**	**67.2**

Only 40.9% of respondents knew the existence of an information security policy. Only 32.8% of participants knew the existence of a password policy.

4.6 Past Experiences of Computer Crime

The open-ended questions of the questionnaire begin by asking the respondents whether or not they have experienced or believed to have experienced computer crime in the past. If the response was yes, they were then asked to provide details of the experience and the actions taken. The purpose of this section is to gain an overview or insight into employee perceptions of any incidents and the actions taken as a result of such incidents.

Only 28 respondents from the sample population of 308 answered yes. Content analysis was performed on these responses and failed to reveal any noteworthy findings relevant for this research. However, various experiences were in relation to phishing attacks. For example, 5 respondents reported experiences relating to credit card theft suggesting that phishing scams are prevalent and highly active. A few experiences were in relation to attempts of hackers to gain access to email accounts. Apart from the credit card scams, there were simply too small a sample set to reveal anything useful.

4.7 Discussion

As can be seen, the results of the questionnaire were both alarming and surprising. Information security awareness as defined by Bulgurcu, Cavusoglu & Benbasat [13] of the employees were generally poor. That is, there was a clear lack of knowledge in terms of information security concepts, as well as generally low levels of consciousness or awareness of policies. The generally low levels of awareness were reflected in employee behaviors, whereby most employees have admitted to performing actions which could have negative consequences for the organization. The ensuing sections discuss in greater detail the findings of this study.

4.7.1 Lack of Knowledge of Security Concepts

The results demonstrated that the organization performed poorly in relation to knowledge of common security concepts(Table.1). The results were particularly poor for social engineering (17.9%). One explanation for the low score could be that social engineering is an ambiguous term in that the terminology is borrowed from the field of political science. Its original meaning relates to governmental influence on society. The term was adopted by the information technology industry to describe the psychological manipulation used by hackers to obtain information [3]. In fact, several respondents complained that none of the available choices for the question reflected their version of what social engineering meant (they used the open-ended sections of the questionnaire to express their concerns). However, given the context (information security) in which the question was asked, it is safe to conclude that they just did not know the answer. Even so, the synonymous nature of the term suggests that the question must be regarded as a limitation of this study.

On the other hand, the organization scored highly in relation to the concept of information integrity (91%). In retrospect, the multiple choices available in the question may have been too obvious for a respondent to hazard a guess. In this case, the core attributes of the concept as defined by Boritz [20] were all options with the subsequent correct answer being "All of the above". Simple logic would suggest that many would guess the correct answer. However, the relatively high score did reflect in the positive results obtained for the question which asked whether or not a respondent have ever amended data without confirming accuracy and correctness. The score was very low (7.8 %), demonstrating that only a small portion of the organization has performed this negative action.

Phishing and spam are concepts which go hand in hand because phishing attacks are often conducted via spam [21]. However, the organization scored relatively high for spam (85.4 %) but very low for phishing (24.7%). Such a large variance may be explained by Bulgurcu, Cavusoglu & Benbasat [13] which suggested that information security awareness in regards to concepts are often built upon life experiences. For example, one may not know of a concept if they have never experienced the phenomenon first-hand. Spam is a tremendously frequent occurrence affecting most people, whereas phishing may not be so obvious until an attack has been committed. Therefore not many people may know the term compared to spam.

It is of the opinion that the organization scored moderately in relation to the concept of a strong password (65.9 %). However, the accuracy of the results must be questioned due to the fact that the initial 308 responses were all subjected to manual content analysis in order to determine whether each response was correct. The manual nature of the analysis in addition to the unlimited variations of open-ended responses raises the possibility of incorrectly classifying each response. This is similar to a University lecturer marking many exam papers. Discrepancies would undoubtedly occur.

4.7.2 Lack of Awareness of Policies

The results of the questionnaire showed that many employees did not know of the existence or the details of the organization's security related policies. Less than half of respondents knew about an actual information security policy (40.9%) and even less for password policy (32.8%). Management performed slightly better, with a score of 59.3% for information security policy and 40.7% for password policy. The most alarming results relate to the general staff, which scored only 36.5% for information security policy and 30.9% for password policy. The poor results suggest that security policies are not well promoted or enforced by the organization and that emphasis is heavily placed on technical controls without taking into account the human aspects of information security. Dzazali, Sulaiman & Zolait [5] suggested that policies or plans become useless if no consideration is given to the human factors of information security. In this case, by not ensuring that employees become proficient in the knowledge of the organization's policies, the policies themselves are futile. The lack of awareness and knowledge of policies may have allowed for staff to violate such policies, as demonstrated and reflected in the results of the behavioral questions summarized in section 4.3. In particularly password based actions, where it was observed that many employees shared passwords, left computer unattended and also used inappropriate methods for password storage. These actions are generally prohibited by an organization's security and password policies if properly enforced. This is not the case for the organization in question.

4.7.3 Lack of Information Security Awareness

Information security awareness is the combination of the knowledge of concepts and awareness of existing policies [13]. Due to the fact that the organization as a whole lack both knowledge of security concepts and awareness of policies as demonstrated by the results, it can be concluded that the employees lack information security awareness. This is in line with the observation made by Knapp et al. [9] that there is a positive relationship between information security awareness and preventative action. That is, employees are more likely to have positive behaviors in relation to information security if their awareness levels are high. In the case of the organization in question, the lack of awareness have resulted in many employees engaging in negative actions and behaviors in violation of information security, thus reaffirming the relationship as defined by Knapp et al. [9].

4.7.4 Relationships between Concepts and Behaviors

The study into the feasibility of a vocabulary test to assess information security awareness conducted by Kruger, Drevin & Steyn [14] identified significant relationships between knowledge of concepts and behaviors. That is, knowing a concept will translate into positive behaviors relating to the concept. However, the current study is in contrast to Kruger, Drevin & Steyn [14]. The results shown in the cross-tabulations between concepts and corresponding behaviors (refer to Table 1) identified surprising results which contradicted Kruger, Drevin & Steyn [14]. For instance, an alarming 74.1% of respondents who knew the concept of phishing still engaged in clicking on links embedded in potential spam. Similarly, an alarming 75.3% of respondents who knew what spam is also engaged in the clicking of links embedded in potential spam. It can be concluded that knowing the concept of spam and phishing did not mean that the employees will not take the risk and click on potentially dangerous links. The likely reason for this may again be attributed to the lack of policy enforcement or promotion.

In relation to strong passwords, the results also contradicted Kruger, Drevin & Steyn [14] in that knowing the concept of a strong password still resulted in staff engaging in password sharing, leaving computers unattended and unlocked. Using the respondents result set as an example, 51.7% of staff who knew what a strong password is did not stop them from sharing passwords. Similarly, an alarming 79.3% of staff who knew the concept of a strong password have admitted to leaving their computer terminals unattended and unlocked. The reason for such actions could be a result of the trust formed between co-workers. However, the security risks are clearly present.

4.7.5 Recommendations

The subject of this study is clearly plagued with employee non-compliance of information security policies. The low levels of awareness may have contributed to such non-compliance. As suggested by Yeo, Rahim & Miri [16], the lack of awareness and non-compliance poses serious risks for the organization and should be properly assessed and mitigated as part of the organization's overall risk assessment strategies. It is therefore highly recommended that the organization implement proper risk assessment strategies which include information security awareness as an important component.

Further, once the security risks are properly assessed, they can be mitigated by improving security awareness. As suggested by Lane [15], the adoption of adequate information security awareness training programs will ensure that employees know of their responsibilities and also foster an organizational culture of information security compliance, thereby improving the mitigation of such risks. It is therefore recommended that the organization explore such programs. The exploration of these programs forms the basis of the suggestion follow up studies in the future.

5. CONCLUSION

5.1 Research Summary

Employee information security awareness has been widely regarded as an important contributing factor in any successful organizational information security plans. However, there is a gap in literature in that very little has been done in an Australian context in relation to information security awareness, thus giving rise to this study.

This exploratory study utilized a specially designed online questionnaire to assess the levels of information security awareness within a South Australian Higher Education Institution.

Information security awareness can be defined as the combination of a person's knowledge of security concepts and the person's awareness or consciousness of the existence of any security related policies. Therefore the questionnaire was used to test the respondents' knowledge of commonly known security concepts as well as the respondents' consciousness of the organizations security policies in order to gain insight into the awareness levels of the organizations. In addition, the questionnaire also tested for behaviors which are related to corresponding security concept.

The results of the study revealed that employee awareness levels for the organization are surprisingly low, with employees lacking in both knowledge of concepts and awareness of the organization's policies. The lack of information security awareness was reflected in the admission by many employees that they had previously engaged in behaviors (such as password sharing) which were in direct violation of information security. This may be a result of the lack of policy promotion and enforcement.

Finally, this exploratory study has achieved the aim of gaining valuable insight into the workings of an Australian organization in relation to information security awareness.

It is important that the organization explore information security awareness as an organizational risk which must be assessed and mitigated. Subsequently, the identified risks may be mitigated by adopting relevant awareness programs which will ultimately foster an organizational wide culture of information security compliance.

5.2 Limitations

Due to time constraints, a full appreciation of the importance of terminologies used in the questionnaire was not realized. For instance, social engineering is an ambiguous term in that it is synonymous with a different meaning within the field of political science. In relation to the responses to strong password, manually conducting content analysis for the relatively large number of responses may have increased the chance for discrepancies.

The initial design of the questionnaire included a question which asked respondents' whether or not they have ever knowingly provided confidential information to outsiders in circumstances they felt it was justified to do so. At the organization's request, the question was omitted from the final version of the questionnaire. The reasoning was that the responses to such a question could potentially create a public outcry for the organization. For instance, if the responses revealed that employees did in fact knowingly released confidential information, the public would have every right to question the organization's integrity. However, by omitting the question, this study may have lost valuable insights.

5.3 Future Research

Assessing information security awareness is deemed to be an initial step in achieving security readiness. The next step would naturally be to determine how the problem areas identified in this study can be approved through best practices. That is, future research should focus on how awareness levels can be improved, thus improving the security readiness of the organization. In the long run, future research should also focus on including information security awareness as part of an overall organizational security strategy by adopting suitable awareness enhancing programs.

6. REFERENCES

[1] von Solms, R 1998, 'Information Security Management (1): Why Information Security is so Important', *Information Management & Computer Security*, vol. 6, no. 4, pp. 174-177.

[2] Cervone, F 2005, 'Understanding The Big Picture So You Can Plan For Network Security', *Computers in Libraries*, vol. 25, no. 3, pp. 10- 15.

[3] Thompson, STC 2006, 'Helping the Hacker? Library Information, Security, and Social Engineering', *Information Technology & Libraries*, vol. 25, no. 4, pp. 222-225.

[4] Cervone, F 2005, 'Understanding The Big Picture So You Can Plan For Network Security', *Computers in Libraries*, vol. 25, no. 3, pp. 10- 15.

[5] Dzazali, S, Sulaiman, A & Zolait, AH 2009, 'Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations', *Government Information Quarterly*, vol. 24, no. 4, pp. 584-593.

[6] Siponen, M & Vance, A 2010, 'Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations', *MIS Quarterly*, vol. 34, no. 3, pp. 487-A12.

[7] Spears, JL & Barki, H 2010, 'User Participation in Information Systems Security Risk Management', *MIS Quarterly*, vol. 34, no. 3, pp. 503-A5.

[8] McFadzean, E, Ezingeard, J & Birchall, D 2007, 'Perception of risk and the strategic impact of existing IT on information security strategy at board level', *Online Information Review*, vol. 31, no. 5, pp. 622-660.

[9] Knapp, KJ, Marshall, TE, Rainer, RK, & Ford, FN 2006, ‘Information security: management's effect on culture and policy’, *Information Management & Computer Security*, vol. 14, no. 1, pp. 24-36.

[10] Mouratidis, H, Jahankhani, H & Nikhoma, MZ 2008, ‘Management versus security specialists: an empirical study on security related perceptions’, *Information Management & Computer Security*, vol. 16, no. 2, pp. 187-205.

[11] Hagen, JM, Albrechtsen, E & Hovden, J 2008, ‘Implementation and effectiveness of organizational information security measures’, *Information Management & Computer Security*, vol. 16, no. 4, pp. 377-397.

[12] Doherty, NF, Anastasakis, L & Fulford, H 2009, ‘The information security policy unpacked: A critical study of the content of university policies’, *International Journal of Information Management*, vol. 29, no. 6, pp. 449-457.

[13] Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010, ‘Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness’, *MIS Quarterly*, vol. 34, no. 3, pp. 523-A7.

[14] Kruger, H, Drevin, L & Steyn, T 2010, ‘A vocabulary test to assess information security awareness,’ *Information Management & Computer Security*, vol. 18, no. 5, pp. 316-327.

[15] Lane, T 2007, ‘Information Security Management in Australian Universities – An Exploratory Analysis’, Faculty of Information Technology Master thesis, Queensland University of Technology.

[16] Yeo, AC, Rahim, M & Miri L 2007, ‘Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution’, in *Proceedings of the Pacific Asia Conference on Information Systems 2007*, Auckland.

[17] Laaksonen, E & Niemimaa M 2011, ‘Information Security Policies, a Frames of Reference Perspective’, Department of Computer Science Master thesis, Lulea University of Technology.

[18] De Haes, S, Van Grembergen, W 2009, ‘An Exploratory study into IT Governance Implementations and its Impact on Business/IT Alignment’, *Information Systems Management*, vol. 26, no. 2, pp. 123-137.

[19] *Microsoft Safety & Security Centre* 2011, Microsoft, viewed 9 October 2011, <http://www.microsoft.com/en-gb/security/online-privacy/passwords-create.aspx>

[20] Boritz, JE 2005, ‘IS Practitioners’ Views on Core Concepts of Information Integrity’, *International Journal of Accounting Information Systems*, vol. 6, no. 4, pp. 260-279.

[21] Whitman, ME & Mattord HJ 2005, *Principles of Information Security*, 2nd edn, Thompson Course Technology, Australia.