International Journal of Research (IJR) e-
ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, June 2015
Available at http://internationaljournalofresearch.org

Role of Information Security Awareness in Success of an Organization

A.M.Chandrashekhar
Assistant Professor Dept. of Computer Science & Engineering, SJCE, Mysore, Karnataka, India
Rahul Kumar Gupta
M.Tech 2nd Semester Dept. of Computer Science & Engineering, SJCE, Mysore, Karnataka, India
Shivaraj H. P.
M.Tech 2nd Semester Dept. of Computer Science & Engineering, SJCE, Mysore, Karnataka, India

Abstract—

Information security (IS) awareness is the very important helping factor for a successful Information Security plan and should be appropriately assessed in order to advise improvements. This explorative study work directly investigated and assessed the employee Information Security awareness levels within a India Higher Education organization for the purpose of providing much needed imminent into the extent of information awareness levels in Indian organizations. Using an online survey, the study revealed that the institute's employee information security awareness were usually lacking. The study also identified several issues in many areas which had abundance for improvements, thus concrete the way for more research into how information security awareness levels can be enhanced. It is recommended that the organization include IS awareness as part of its overall risk review strategies in order to moderate such risks.

Keywords— Information Security; Information Security Awareness

I. INTRODUCTION

Due to advance in information technology and the consequential high ability and accessibility of information by internal and external users, Information Security has become more relevant and necessary for the survival of organizations[1]. Failure to protect secret information may result in very expensive costs in public liabilities, which may result in the crucial downfall of an organization. There are three significant aspects of Information Security[2]. First aspect relates to preventing unauthorized access of information, thus ensuring that confidential data well protected. Second integrity relates to the exactness and currency of information, thus ensuring that information is reliable and realistically represents the real world in which the data is based on. Thirdly, availability of information relates to authorized access of information or data are provided when required. The main purpose of IS, is to ensure business stability in order to minimize damage and responsibility to the organization. Furthermore, institutes have both an ethical and authorized responsibility in ensuring that secret information is well protected[2].

The objective of this paper is to minimize the risk of information security breaches it is important for an institutes to implement an IS strategy. IS measures frequently consist of utilizing technical controls in order to moderate Information Security risks. However, the paper stated that technical controls become unsuccessful if the people interacting with the data or information systems do not have sensible security practices.

Information security awareness is an employee's awareness of information security concepts and his or her awareness of the organization's information security plans. Due to the clear gap which exists in recent literature in that studies in relation to organizational IS awareness in an Indian situation are minimal, this exploratory study aims to assess the employee knowledge of an Indian organization.

II. BACKGROUND

The following sections present a review of existing literature relating to IS awareness and within the scope of this study

A. Need for Information policy

IS awareness as an employee's familiarity of information security and his or her awareness of the

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, May 2015
Available at http://internationaljournalofresearch.org

organization's IS measures or plans. One paper define employee reasonability based behaviors, information security awareness, and their special effects on Information Security compliance. The study gave the over view to show that an employee's objective to obey is greatly influenced by employee's attitude and their outcome beliefs. More importantly for the purpose of this survey, the study come out with that an employee's thoughts and outcome beliefs are exaggerated by their level of Information Security awareness.

B. Maintaining the Integrity of the Specifications

It is important to study existing literature on supervisory information security awareness. McFadzean, Ezingeard & Birchall [3] the awareness of higher authority management as an important part of effective security measures. The study defined that senior person have a good view of the organization. Therefore have the authority to affect change in the organization through their roles as policy implementers. Similar to this one paper also define senior management as key player. The study found that higher-ranking management support is absolutely related to an organization's security culture and the level of strategy enforcement. While the study did not exploring decision-making information security awareness on security performance, it did again emphasize the importance of management contribution, thus the importance of supervisory information security awareness in disturbing an organization's information security readiness.

There is no so much information security awareness within common management and as mention this could have a harmful impact on the effectiveness of information security strategies.

C. Assessing ISA

In determining a helpful relationship between information security awareness, employee rationality based behaviors and policy compliance, Bulgurcu, Cavusoglu & Benbasat [4] three simple questions in set of questions to gauge security awareness. These questions are:

1. I know the rules and regulations arranged 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 define in the ISP to enhance the IS of my organization.

As we 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. The questions were again limited in that they were only relevant in the context of an existing security policy.

To overcome the limitation of information security awareness most general tool for assessing information security awareness. Similarly, the study by Namjoo et al. [5], conclude that an organization's survival necessitates a security program. Due to the importance of information security awareness in ensuring a successful plan, the study will be adapted to fit the Indian organizational context and will be taken to use to assess awareness levels of organization's employees in question. A Security Education, Training and Awareness (SETA) program can be clear defined as an educational program that is planned to reduce the number of security breaches that occur through a lack of employee security awareness. A SETA program sets the security rule for the employees of an organization, particularly if it is made part of the employee orientation. Awareness programs give details the employee's role in the area of Information Security. The aim of a security awareness effort is participation. Technology alone cannot solve a problem that is controlled by individuals. A SETA awareness programs give details the organization employee's role in the area of Information Security. They show the users where they can play a very important part in the protection of the organization's information. They serve to instill a sense of responsibility and purpose in employees who handle and manage information, and motivate to employees to care more about their work environment.

III. METHODOLOGY

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

A. Aim

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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, May 2015
Available at http://internationaljournalofresearch.org

B. Research Methods

The nature of this research is exploratory rather than to test for hypothesis. According to Ryerson, cited in De Haes & Van Grembergen, 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.

C Set of questions Justification

A set of questions was used for this explorative study because a related study has proven the use of such set of questionss in assessing information awareness to be both beneficial and practical [6].

An online set of questions 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 set of questions ensures a greater reach and better response rates. The set of questions requires about ten minutes of the respondent's time for completion and the resulting collected data is immediately available.

IV. SET OF QUESTIONS DESIGN

The set of questions 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 set of questions 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 set of questions design and the set of questions can be found in Appendix A.

A. Section 1 – Knowledge of Concepts

Similar to Kruger, Drevin & Steyn [6], Various generally known or common concepts identified in the literature review were included in this section of the set of questions 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 "bonnets" or "Steganography"[6]. 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

B. Section 2 – Employee Behaviors and Actions

Common concepts identified in the literature review were included in this section of the set of questions 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 "bonnets.

C. Section 3 – Consciousness of Policies

This section of the set of questions relates to the second part of the definition of information security awareness. 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.

V. DATA COLLECTION

The online set of questions was created and deployed using the web-based survey service provider Qualtrics was selected for the task because

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, May 2015
Available at http://internationaljournalofresearch.org

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 set of questions 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 set of questions, consent was thereby simultaneously given by the respondents.

The use of an online set of questions ensures a higher rate of responses compared with traditional paper based surveys due to its convenience for respondents. The design of the set of questions itself is based on principles used in similar studies which have proven to be both practical and beneficial. The results of the set of questions will be presented in the ensuing.

VI. RESULTS

The online set of questions was distributed to all employees of the organization in question. There are approximately 2000 employees, equating to a population of 2000 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 set of questions.

A. Demographics

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

B. 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 [7] 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
Phishing	Yes No	70 245
Spam	Yes No	283 42
Social Engineering	Yes No	45 283
Strong Password	Yes No	213 95
Information Integrity	Yes No	281 27

Only 24.7% of respondents knew the term phishing. 35% of respondents knew what spam is. Only 15.5% of respondents knew the term social engineering. 72% of respondents had an idea of what a strong password should be. 95.3% of respondents knew the importance of information integrity.

C. Employee Behaviors

Table 2 presents and summarizes the results of section 2 of the set of questions.

Table 2. Employee Behaviors

Action	Performed Action	Responses
Given away passwords or logged someone on using own password	Yes No	183 123
Left computer unattended and unlocked	Yes No	218 70
Used inappropriate methods for storing passwords	Yes No	105 203
Clicked on unknown links embedded in third party emails	Yes No	228 80
Amended data without confirming accuracy or authenticity	Yes No	24 284
Disclosed work related information on social networking sites	Yes No	23 285

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, May 2015
Available at http://internationaljournalofresearch.org

A surprising 55.3% of respondents have given away passwords or logged someone onto a computer using their own password. A surprising 78.6% of respondents have left their computer unattended and unlocked. 38.4% of respondents used inappropriate methods for storing passwords. A surprising 78% of respondents have clicked on unknown links embedded in third party emails. Only 8.8% of respondents have amended data without confirming accuracy or authenticity. Only 6.5% of respondents have disclosed work related information on social media.

D. Relationships between Concepts and Behaviors

Surprisingly, 81.3% of respondents who knew the meaning of phishing still clicked on unknown embedded links. Similarly, 78.3% of respondents who knew the meaning of spam still clicked on unknown embedded links.

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	155	50
	Percentage	75.1	18.6
Did not know what phishing is	Responses	65	10
	Percentage	85.5	28.6
Knew what spam is	Responses	188	55
	Percentage	65.6	22.8
Did not know what spam is	Responses	35	18
	Percentage	75.2	31.6

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**	115	55.6	45	45.5
	No	78	38.6	45	45.6
Has left computer unattended and unlocked	**Yes**	178	83.2	65	71.9
	No	38	19.6	22	35.7
Has used inappropriate methods for storing passwords	**Yes**	81	39	48	37.5
	No	125	85	55	54.6

45.5% of respondents who knew the concept of a strong password have admitted to giving away their passwords. 71.9% of respondents who knew the concept of a strong password have admitted to leaving their computers unattended and unlocked. 37.5% 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	41	280
	Percentage	11.5%	88.5%
Did not know the importance of information integrity	Responses	3	24
	Percentage	19.8%	75.9%

11% of respondents who understood the importance of information integrity have amended data without confirmation or due process.

E. Consciousness of Policies

This section presents and summarizes the results of section 3 of the set of questions 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**	**116**	**38.8**
	No	**170**	**56.7**
Password Policy	**Yes**	**112**	**35.8**
	No	**197**	**73.2**

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 06, May 2015
Available at http://internationaljournalofresearch.org

Only 38.8% of respondents knew the existence of an information security policy. Only 35.8% of participants knew the existence of a password policy.

F. Past Experiences of Computer Crime

The open-ended questions of the set of questions 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.

G. Discussion

As can be seen, the results of the set of questions were both alarming and surprising. Information security awareness as defined by Bulgurcu, Cavusoglu & Benbasat [4] 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.

a) 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. 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 [8]. 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 set of questions 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.

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 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.

b) Lack of Awareness of Policies

The results of the set of questions 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 [8] suggested 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 C.

c) Lack of Information Security Awareness

Information security awareness is the combination of the knowledge of concepts and awareness of existing policies [4]. 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 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.Deletion: Delete the author and affiliation lines for the second affiliation.

D) Relationships between Concepts and Behaviors

The study into the feasibility of a vocabulary test to assess information security awareness conducted by Kruger, Drevin & Steyn [6] identified significant relationships between knowledge of concepts and behaviors. That is, knowing a concept will translate into positive behaviors relating to the concept. The results shown in the cross-tabulations between concepts and corresponding behaviors (refer to Table 1) identified surprising results

In relation to strong passwords, the results also contradicted 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, 95.3% 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.

e) 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 [8], 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. 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.

VII. CONCLUSION

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 Indian context in relation to information security awareness, thus giving rise to this study. This exploratory study utilized a specially designed online set of questions to assess the levels of information security awareness within a South Indian Higher Education Institution.

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. Finally, this exploratory study has achieved the aim of gaining valuable insight into the workings of an Indian 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.

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] 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.

[4] 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.

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

[6] 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.

[7] 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.

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

[9] Hong chan and sameera mubarak. 'Significant of information security awareness in the higher education sector' vol.60 no. 10 december 2012.