

# A Conceptual Model To Understand Information Security Awareness

S. Bharathi<sup>1</sup>

Assistant Professor

Department of Computer Applications  
Vellalar College for Women (Autonomous)  
Thindal, Erode - 638 012, Tamilnadu, India

Dr. J. Suguna<sup>2</sup>

Associate Professor

Department of Computer Science  
Vellalar College for Women (Autonomous)  
Thindal, Erode - 638 012, Tamilnadu, India

**Abstract**— Information technology plays an important role in everyday lives and it affects the status of information security. Commonly used meaning for information security in literature is the preservation of confidentiality, integrity and availability. The main aim of the research is to examine the information security awareness and influence information security culture through awareness before applying to any organization. Information security awareness provides some kind of safeguard for our information from outside attack. Most of the security incidents are occurred due to the negligence and unawareness of the users. It is important for all employees in society to keep the awareness of information security at higher level. Generally few users with poor awareness and many users with rich awareness of information security in society exist. End-users attitude and the evaluation of information security policy are the two important factors in raising information security awareness. The success of project management within organization requires security awareness. This paper proposes an information security awareness model (ISAM) which analyzes and identifies the most common events related to information security awareness and categorizes these events as low-level, mid-level, and high-level.

**Keywords**— Information Security; Security Awareness; ISAM; Information Security Awareness Model;

## I. INTRODUCTION

An information security awareness program provides financial benefits to many organizations. Major benefits include organizations information security performance, values, beliefs, attitude and action of the organization members. All the users are responsible for the protection of information; it is not only the responsibility of information security people of the company. Information security means protecting information and information systems from unauthorized access, unauthorized use and disclosure. Many of the organization and Universities are still vulnerable from human attitude threats.

Information security awareness can be defined as, Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and responds accordingly.

Security awareness [2] is the knowledge and protection of the physical and intellectual property of an organization. Many organizations require formal security awareness training for

all workers when they join the organization and periodically thereafter, usually annually.

There are lots of risks and threats that affect the proper functioning of information systems, which result from the rapid technological developments and technical problems, rapid communications, environment change, political and economic problems and human weakness. So the growing subject of information security leads to information security awareness. Protection of information resources requires a well-designed policy, helpful guidelines and brand name. Information security and ethics awareness became one of the most popular topics discussed in IT and business circles today. The objective of the proposed model includes,

- Review of the existing frameworks. Summary of proposed constructs from the existing studies.
- Findings from the studies and give rankings according to their citations.
- Develop a new conceptual model for awareness.

## II. LITERATURE REVIEW

Model for information security service branding (ISSB) [8] represents and create a positive brand image for information security. The information security service branding include the definition of information security service brand, communicating the brand to end-users, organizing the brand to deliver security culture, monitoring end-users perception of information security service brand and end-users characteristics. This paper discusses the importance and weakness of information security awareness. Knowledge management tool [12] was found and it can be used to enhance the information security. Knowledge management includes three major phases namely knowledge capture and/or creations, knowledge sharing and dissemination, knowledge acquisition and application. To improve information security number of knowledge management tools were used.

Phishing experiment was conducted at the American university of Sharjah [3] in UAE among the students, faculty and staff. The experiment was performed within thousand faculty and staff, five hundred students and five thousand alumni. A website was setup at the end of the experiment,

explaining the details of the experiment, the results showed the necessity of security awareness training and after the experiment the victims became more aware of phishing attacks. Two weeks later another phishing audit was conducted to analyze the awareness. After the awareness campaigns number of victims are dropped from 9% to 2%. The framework [9] includes various features which will be helpful to protect information and information systems from an unauthorized access. This framework was developed for information security policy and it consists of some features or all features of some existing information security policy and it provides high class security with reliability.

Kiran Kumar Kommineni et al., [6] presented an incremental approach for the assessment of enterprise information security. The proposed approach has three levels and is based on the TOPE scope and ISO/IEC 27002 standard. Level one includes the essential and common security measures. Level two includes the ISO/IEC 27002 security measures. Level three includes the ISO and other security standards. Toshihiko Takemura [11] analyzes Japanese workers awareness to information security using the data collected through the web-based survey in March 2009. He developed a hypothesis for the attributes of working pattern, organization and individual attributes namely H1, H2 and H3. By running analysis of variance the average value and the median of the groups can be verified and that offer motivation and prohibit certain countermeasures.

This study [1] consists of two kinds of data that is primary and secondary data. The primary data was gathered through a questionnaire survey and direct interview. The secondary data was collected from journal, text book, articles, conference paper, reports and documents that published. The main objective of this paper was to anticipate the risk through access of user level awareness. The variables learnability, adaptability and performance are observed through the roles of responsibility. Various dimensions [10] of information security awareness which includes organizational, socio-political, computer ethical and institutional education dimensions are discussed in this paper.

C. Banerjee et al., [2] created security awareness among software development team right from the beginning. So that they proposed the improvised software security awareness model. A questionnaire [5] survey was conducted in a large sized bank in Greece which includes two hundred and twenty seven employees. The questions analyze the different components of information security.

The authors [7] examine the level of ethical and security awareness among IT students. Satisfactory level of awareness among IT students was found out in this survey. Through the questionnaire survey they found that the female students are more conscious about security and ethics awareness when compared to male students.

### III. DEVELOPMENT OF CONCEPTUAL MODEL

To construct an information security awareness model, an understanding of existing awareness models and frameworks are essential. A review of the existing frameworks and security awareness measures are essential to develop a new conceptual model. The comprehensive review of information

security awareness and framework was conducted and based on the identification and the findings of the review; proposed an information security awareness model. The objective and constructs of each study in the information security area leads to develop a conceptual model. This review has also includes a questionnaire assessment of information security to assist in the development of information security awareness model.

TABLE I: SUMMARY OF PROPOSED CONSTRUCTS IN INFORMATION SECURITY AWARENESS RESEARCH

Author	Objective	Constructs
Ragul Rastogi [8]	Creating the information security service brand.	Information security management; Information security service management; Brand Awareness; Service management; Information security service Branding, Security Policy, ISSB, Service Branding.
Yogesh Kumar Mttal, Dr.Santanu Roy and Dr.Manu Saxena [12]	To enhance the information security various Knowledge management tools are used.	Content management, Knowledge Management, Groupware, Online communities of practice, Enterprise portal, Social network analysis and design, E-learning, Storytelling and Narrations, Wireless tools for knowledge mobilization, Innovation and idea management system, Tools for extending KM across organizational boundaries.
Fadi A. Aloul [3]	The need for security awareness program in the middle east, UAE.	Information security; security Awareness; Security Audits; Phishing Attacks; Wireless Security.
Satish Kumar Er.,Amit Puri [9]	To propose a new framework for information security and it should provide better security.	<b>Organize the analysis chart:</b> Information security policy; Authorized person's name; Designation; date and time; policy name; policy parameter; overall policy rating. <b>Designing of a new framework:</b> Security policy; framework; Risk. <b>Simulating the proposed framework:</b> Simulator; Security policy. <b>Evaluation and Validation of the proposed framework:</b> Simulator; Security policy.
Kiran Kumar Kommineni, Adimulam Yesu Babu [6]	Identification of set of assessment measures.	Information Security; Risk Management; Assessment. <b>Level 1:</b> Essential security <b>Level 2:</b> Base-line security <b>Level 3:</b> Detailed security
Toshihiko Takemura [11]	Quantitatively analyze the Japanese workers awareness to information security.	Information security; Awareness; Worker; Analysis of Variance (ANOVA); Knowledge management, Web-based survey methods.
Abdul Rahman Ahlan, Muharman Lubis [1]	To anticipate the risk through user level awareness.	Information security Awareness; Learn ability; Adaptability; Performance; Roles of responsibility; Wireless policy.
Mikko T.Siponen	Outlines the dimensions of	Organizational dimension; general public dimension;

[10]	information security awareness along with their categories.	Socio-public dimension; Computer ethical dimension; Institutional educational dimension.
Banerjee C., Arpita Banerjee, Murarka P.D [2]	Create an improvised software security awareness model.	Software Security; Security Awareness; Software Security Awareness Method; Improvised Software security Awareness models; ISSAM; Methods, Policies; Awareness Campaigns; training and education.
Ioannis Koskosas, Nikolas Sariannidis, nikolaos Asimopoulos [5]	To investigate project commitment in the information systems security.	Project Commitment; Risk Perception; Organizational Business Goals; Information Security Management Process.
Mansur Aliyu [7]	To examine the level of ethical and security awareness among IT and education students.	Computer security; Computer ethics; education; information technology, Security Policy.

The main purpose of this review is to construct a conceptual model for information security awareness through the findings of the review. Table I summarizes the list of objectives and the constructs for each study. The first column represents the author's name and the second column represents the objective of each study. The third column represents the constructs for each study in the review of the information security framework.

Eleven studies were observed in Table I. The purpose of the proposed construct was to examine the level of the awareness in the field of information security. From Table I, the proposed constructs were counted and listed in Table II in order to develop a conceptual model for information security awareness model. The conceptual model for awareness of information security is developed based on the rankings of Table II.

TABLE II: CONSTRUCT LEVEL IN THE INFORMATION SECURITY AWARENESS RESEARCH

S.No	Constructs	Number of times cited out of 11 studies	Rankings
1	Training	2	1
2	Responsibility	2	3
3	Brand	2	4
4	Campaigns	2	2
5	Education	3	1
6	Methods	3	2
7	Policy	5	1
8	Knowledge Management	5	2

The model for awareness of information security is classified into three major levels namely high-level, middle-level and low-level as shown in Fig.1.

Broadly examined factors are counted for the proposed development model. The top constructs are classified under the high-level, middle-level and low-level because it is

impossible to examine every factor which could help in the conceptualization.

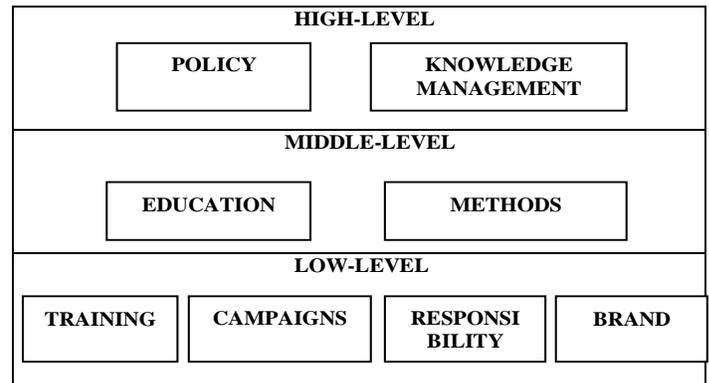


Fig.1 Conceptual model for Information Security Awareness

From Fig.1 security awareness is part of any organization's information security. Every organization's information security depends on the external and internal factors. Through the proper awareness solution organization's informations and information systems are preserved from inside and outside threats.

Information security policy mainly focuses on information management and training on general staff. Information security policies should be promoted in a top-down manner to meet the requirements and it should be reviewed at planned intervals. Because of the lack of awareness about the importance of information security among students and staff in the organization the policies are often reviewed to protect the information.

Knowledge management helps individual people to do their job in an efficient way through better decision making and problem solving. This will be helpful to keep people up to date and minimize the opportunities for computer fraud. In an organization level, users become upgraded when their experience and knowledge were shared. Knowledge management will encourage people to give new ideas and innovations and rewarding them accordingly.

Development of information security model needs to be educating people. The information security training and awareness program covers recent issues in information security and needs motivations to improve and enhance the awareness about information security.

Organizations need to work consciously towards creating a brand image. Positive brand image leads to organizations gain and negative brand image leads to bad impression in users mind. Information security methods are used to protect the information from unauthorized access. Methods are derived in order to understand the principles and rules of different situations.

The responsibility covers how an individual handle information carefully and must be trained to become aware of the loopholes. The development of information security awareness needs the combination of training and campaigning to increase the understanding of information security.

#### IV. CONCLUSION AND FUTURE WORK

Lack of awareness and less priorities about information security leads to this information security awareness model. This model identifies the further actionable step for the improvement of the society. Information security awareness should be the first priority in the development of Internet service providers. The existing literature review provides suggestions and guidelines on how to prevent our Information's from the external and internal factors. These literature analyses have not provided a clear idea or understanding to develop a conceptual model. This is an initiative to identify what factors constitute a conceptual awareness model. The proposed model influences the order of security awareness. The high-level constructs are better than the low-level constructs and this may be helpful to the organization to concentrate more on low-level. In order to achieve this goal, questionnaire survey will be conducted to develop the information security awareness model in organizations. Additionally qualitative interviews will also be included to identify the awareness. These will assist to minimize the external factors which will affect the security awareness. This is not implemented in any organization or university. The implementation of this model would be the future work of this paper. During the implementation the rankings and the constructs place might be changed depending on the organization.

#### REFERENCES

- [1] Abdul Rahman Ahlan, Muhamman Lubis, "Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility", in proceedings of 7 th International Conference on Information Assurance and Security, IAS 2011, Melacca Malaysia, December 5-8, 2011.
- [2] Banerjee C., Arpita Banerjee, Murarka P.D., "An Improvised Software Security Awareness Model", International Journal of Information, Communication and Computing Technology, Jagan Institute of Management Studies, New Delhi, Vol I, Issue II(July-Dec2013):ISSN 2347-7202.
- [3] Fadi A.Aloul, "The Need for Effective Information security Awareness", Journal of Advances in Information Technology, Vol. 3, No.3, August 2012.
- [4] Hallvard Kjorvik, "Implementing and Improving Awareness in Information Security", Thesis, University of Agder.
- [5] Ioannis Koskosas, Nikolas Sariannidis, nikolaos Asimopoulos, "A Survey in Project Commitment in the Context of Information Security", Journal of Emerging Trends in Computing and Information Sciences, Volume 2, No 2, ISSN 2079-8407.
- [6] Kiran Kumar Kommineni, Adimulam Yesu Babu, "An approach for the Assessment of the Information Security and Its Measures", International Journal of Soft Computing and Engineering(IJSCE), Volume 3, Issue-1, March 2013, ISSN:2231-2307.
- [7] Mansur Aliyu, Nahel A.O.Abdallah, Norjeem A.Lasisi, Dahir Diyar, and Ahmed M.Zeki, "Computer Security and Ethics Awareness among IIUM Students: An Empirical Study.
- [8] Ragul Rastogi, Rossouw von Solms,"Information Security Service Branding-beyond information security awareness", Systemics, Cybernetics and Informatics, Volume 10, No.6, 2012, ISSN:1690-4524.
- [9] Satish Kumar Er.,Amit Puri, "A Framework for Evaluation and Validation of Information Security Policy", International Journal of Computers and Distributed Systems, Vol.No.1, Issue 3, October 2012, ISSN: 2278-5183.
- [10] Siponen T. Mikko, "Five Dimensions of Information Security Awareness", Computers and Society, June 2001.
- [11] Toshihiko Takemura, "A Quantitative Study on Japanese Worker's Awareness to Information Security Using the Data Collected by Web-Based Survey", American Journal of Economics and Business Administration 2(1):20-26,2010, ISSN:1945-5488.
- [12] Yogesh Kumar Mttal, Dr.Santanu Roy and Dr.Manu Saxena, "Role of Knowledge Management in Enhancing Information security", International Journal of Computer Science, Issues, Vol. 7, November 2010, ISSN: 1694-0814.