**Saudi Journal of Business and Management Studies (SJBMS)** **ISSN 2415-6663 (Print)**
Scholars Middle East Publishers **ISSN 2415-6671 (Online)**
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

# Information Security Awareness and Training in the Digital World

**Lina Maria Dias E Fernandes**
Writing Consultant, Writing Center, Sultan Qaboos University, Sultanate of Oman

***Corresponding author**
*Lina Maria Dias E Fernandes*

**Article History**
*Received: 10.01.2018*
*Accepted: 20.01.2018*
*Published: 30.01.2018*

**DOI:**
10.21276/sjbms.2018.3.1.8

**Abstract:** In the era of digital technology, technology has developed rapidly however the information technology security lags drastically. There has been increase in risk and threats to the organization's information. For every organization, information is a valuable asset and therefore has to be kept safe and secured. Employees are mainly responsible for security risks and threats. Organizations should give attention to the common vulnerabilities and mistakes which employees tend to make and moreover these should be addressed through awareness training programs. Information security awareness training is essential for every organization that uses technology. The study explores the importance of information security awareness training and the challenges faced by organizations is implementation of information security awareness training program. Information security training program protects the confidentiality, integrity and availability of the organization information. This study will assist management to provide effective security awareness training to technology users and enhance the safety and security of information.

**Keywords:** awareness, employee, information, technology, training, security.

## INTRODUCTION

Technology has brought development and transformation of business. With the increased use of smart technologies in business we can only expect increase in the risks and threats to information security. Many organizations are continuously trying to improve the safety and security of information; however such efforts are not adequate and they suffer from financial losses as millions of records are stolen [1].

The article Best Practices for Implementing a Security Awareness Program [2] claims that the cause of risks to organization is due to the action and inaction of employees. The employees and also subcontractors, partner and third parties who have access to information system are a threat and risk to an organization's information. Information security awareness and training provides the required skills and competencies in order to mitigate and decrease risk and threats to information.

The threat to information security is mostly within the organization (CTG 2008). Most organizations believe that technology on its own will safeguard the information against security risks and threats, and they fail to understand that it is the people working for the organization who are the employees are mainly responsible for security risks and threats [3]. If the employees do not have the required knowledge and understanding of keeping an organization's information safe and secured then there are chances of information being inappropriately handled and used by employees and unauthorized person. In addition to this it would result to noncompliance of the information security policies and procedures. Information security is highly important for the success and reputation of organization.

With the development of the new technology there has been an increase in the use of new gadgets like smart phones, tablets and laptops with internet at workplace. The technology has developed rapidly however security lags drastically. Organizations should give attention to the common vulnerabilities and mistakes which employees tend to make and moreover these should be addressed through awareness training to employees (CSI (2010/12). Educating the users of information technology would prevent a lot of problems of information security. According 2017 Insider Threat Intelligence Report [4], 74 percent of the vulnerabilities comes from inside the organization out of which 7 percent are dangerous vulnerability. Though most organizations have a security program in place, the comprehensive changes to the internet is challenging and could threaten if timely action is not taken. Hence it is necessary to train employees in handling information security and educating them on possible risks and threats to information. Such training must be delivered to all employees in the organization in a timely and efficient way.

The study aim is to focus attention to the importance of information security awareness training and the challenges faced by organizations in implementation of information security awareness training program. For the purpose of study, the data is collected from published journals, articles, reports and books on information security awareness training.

## WHY INFORMATION SECURITY AWARENESS AND TRAINING NEEDED

Information security awareness and training for employees is vital and must be done on a regular basis. It is the responsibility of the management to ensure that the employees do not make errors or frauds that would lead to financial loss. Security awareness program educates the employees on security policies and procedures and risk and threats to information thereby reducing financial loss. Moreover, information security training program protects the confidentiality, integrity and availability of the organization information. Confidentiality educates users of the technology to protect and prevent unauthorized disclose of information. Integrity ensures that no unauthorized modification made to information internally and externally while availability makes the information available to the required people when needed.

Ramalingam *et al.* [5] conducted research study amidst the education institutions in Oman and explored the level of Information Security awareness among staff and students of the institutes. This study concluded information security training and awareness program was necessary in order to give knowledge to the staff on information security policies, procedures and reporting of threats. They argued that for an effective information security practice and procedures is essential to give importance to Information Security awareness.

It is important and essential for an organization to have a recognized security awareness program to assist in educating, monitoring and maintaining of security awareness program and should be an ongoing program (PCI SSC, [6]). Such a training program is essential for all personnel of the organization. The best practice is to appoint a security awareness team in the organization and assign responsibilities, develop appropriate content for the security awareness program and create checklist for the purpose. Information security awareness training program will enhance the employee's knowledge of the importance of protecting sensitive information (PCI SSC, [6]).

Herold [7] stated that it is important to educate employees on information security and privacy. The listed reasons are:

- There are numerous laws and regulations to be followed by an organization and these need proper training and awareness of employees' action inside the organizations.
- For maintaining customer satisfaction by keeping their personal information safe and secured. Proper training of disposal off and protecting their information.
- For compliance with policies of information security and privacy policies.
- To eliminate and reduce illegal actions by implementing an ethics and awareness program that educates employees with compliance to relevant laws.
- Maintaining the company's reputation and reducing the risks to private information and keeping it safe from media attention and reporting by awareness and training program

In recent years most of the management primarily focuses on people for security of information rather than technology [3]. People refer to employees in the organization and they must be educated and trained about the security of Information. The success of information security in the organization mainly depends on effective compliance of Information security policies by all users [3]. These can be achieved by the management through security awareness among employees.

Brondie [8] overviews on the importance of training and the training methods for raising information security awareness. She claimed that the training and awareness program for the employees will help to avoid costly errors of security to information and also provide useful information to users in handling risks and threats. Brondie suggested awareness and training on information security is not just the best method, moreover it is very helpful to employees to get a good understanding of information security policies, guidelines sand procedures.

Information security awareness aims is to focus attention on information security of the user in the organization [9]. The objective is to draw the users' attention to information security issues and respond accordingly. Wilson & Harsh [9] define the term 'Training' as level of relevant learning required acquiring the security skills and competencies in managing Information security to individuals. The difference between the two is that training intends to show the required skills, allowing individuals to perform a particular function, while awareness focuses on an attention of an individual on problem i.e. threats and risks. The skills obtained by an individual from the training are based on the awareness.

## OBSTACLES OF INFORMATION AWARENESS TRAINING

Organizations face obstacles in implementing a successful information security awareness training program. The main problem faced is the role of compliance by the employees. Most of the users are under the perception that information security is not their task but a sole responsibility of the information security personnel. However, it is important that all staff understand that everyone in the organization have the responsibility to maintain information security. Just by having the best of policies documented would be useless if the people in the organization are not aware of them, sometimes there is lack of understanding and compliance of these security policies and procedures for lack of proper training.

It is essential for adherence to the security policies and procedures. The employee's action or inaction can lead to security incidents. Some of the organizations may face difficulty in dealing with safety of information as many employees do not understand the importance to protect information, although the organizations may conduct security awareness and training programs on regular basis or it could be that, some of the employees are under the impression that security of information is the duty of the Information Technology department. It could be that the security information program is newly implemented and the employees find it challenging or it could be that too much of information is given during the training program.

Achieving complete security compliance is a big challenge to the Management. It is not possible to achieve full compliance though the management does their best to encourage employees to comply with the security policies and procedures. Inside threat accounts for 43 percent of data loss from those companies that experienced breach of data (Tara Seals 2015). Puhakainen [10] explored how user's information security behavior can be improved and he claimed that the behavior of the users is an important factor that leads to either positive or negative behavior. According to him the negative factor was that following the information security policies and procedures may reduce the speed of work however saving time could result in risk to information.

It is not an easy task to provide meaningful and useful information security awareness training to the staff. A security programs designed to fit all employees in the organization is most likely to fail in delivering the required message to audience. Information security professionals adopt such a method of delivery as it makes their jobs easy however not very effective. The effect of such general security training program could result in trained employees who are threat and risk to the information security

The cost of developing security awareness training program is relatively high. In most of the organizations the security programmers find it challenging to get management approval and funds for the program. Developing and implement security awareness may look complicated, time consuming and costly [11]. Though process is expensive and costly, in the long run it is worth it as it helps to mitigate and reduce risk and threat to information. The program would be ineffective and expensive only when the employees fail to understand their role in the security plan [12]. Moreover, many organizations are not aware that the losses prevent by security awareness training program are much higher than the cost.

## IMPLICATION FOR EFFECTIVE INFORMATION SECURITY AWARENESS TRAINING

Awareness and training very helpful to employees for they get a good understanding of information security policies, guidelines and procedures on information security and thus the best method for keeping information safe and secured [8]. A good security awareness program offers employees the required knowledge for the protection of organisation sensitive information and thus enables to have positive attitude towards security [12].

Information security awareness training, newsletters articles, campaigns, video games, e-mail messaging and posters can be used from time to time to provide employee's information on emerging threats, newly discovered viruses, computer incidents and guidelines for actions [13]. Posters and email messaging can be used for delivering short messages like reminders on safety actions. Such methods have positive effect on manager's and employee's attitude and their behaviour which benefits the organisation. It also helps provide employees, information on current events of security attack to information and hence possible to avoid risk of harm, suspect breaches and take timely action against breaches. Khan *et al.* [13] study showed information security awareness and training along with other methods can be made effective with an increase in information security knowledge of employees and behavioural change of the employees for the protection of information

The security awareness training program must be held on regular basis to different groups of employee's e.g. new employees, existing employees, personnel, Information technology specialist and security staff [14]. Different methods such as, lecture-based and interactive learning, creating security awareness website and visual aids for helpful hints and tips can be used to provide security training for employees [8]. The content should be not too lengthy but precise and engaging as this would help the employees to remember. Some of the areas to be included on training: usage and management of password, protection of computers and data from worms, viruses, Trojan horses, and other malicious software, visitor access and space restrictions, information security policies, guidelines and procedures, backup and storage of Information and email etiquette [9]. It should focus on what has to be done to keep information safe rather than the 'don'ts'.

Information security personnel should take care to see that the training program provide the employees complete knowledge and understanding required to keep organization's information safe and secured.

Every employee in the organisation that is those using and those not using digital devices for work has roles and responsibility towards information security. The security awareness and training program should be an on-going program that fits in the culture of the organization. It should include continuous training, timely communication and support to users of technology. Annually conducted training programs may serve to be inadequate as it would not be able to provide information on the new risk and threats. Training material for security awareness training program may be developed by professional from within the organization or outsourced to develop or bought from vendors (PCI SSC, [6]). The available resources, time and culture of the organization should be considered when choosing the material for security awareness program.

## CONCLUSION

In this digital world of technology every organization must build an information security awareness culture. The success of information security not only relies on development and implementation of security policies and security controls, but moreover on compliance to the security policies by the employees. Therefore, security awareness and training programs should be conducted regularly along with regular security audits. This would enable organizations to maintain confidentiality of financial data, personal information of employees. Customers, investors and other members, reduce information security threats and risks, and minimize financial losses

The study shows the importance information security awareness training and the obstacles faced by the organisations. It then defines the implication for organisation for an effective information security awareness training for the employees.

The current research findings proposed for future research in several directions. The study provided an insight on the importance security awareness and training and difficulties faced by the organisation in security awareness training the employees. There is a need for empirical study focusing on information security awareness training issues faced by banks, hospitals and educational institutions. This study has laid a good foundation for further research.

## REFERENCE

1. Howarth, F. (2015). The Damage of a Security Breach: Financial Institutions Face Monetary, Reputational Losses. Retrieved October 27, 2016, from https://securityintelligence.com/the-damage-of-a-security-breach-financial-institutions-face-monetary-reputational-losses/
2. Best Practices for Implementing a Security Awareness Program. (2014). Retrieved December 9, 2017, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
3. Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information security technical report*, *14*(4), 223-229.
4. 2017 Insider Threat Intelligence Report. (2017) Retrieved December 23, 2017, from https://dtexsystems.com/2017-insider-threat-intelligence-report/
5. Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. *arXiv preprint arXiv:1602.06510*.
6. PCI Security Standards Council (PCI SSC) (2014). *Best Practices for Implementing a Security Awareness Program.* Retrieved March 21, 2017, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
7. Herold, R. (2010). *Managing an information security and privacy awareness and training program*. CRC press.
8. Brodie, C. (2008). The importance of security awareness training.
9. Wilson, M., & Hash, J. (2003). SP 800-50. Building an Information Technology Security Awareness and Training Program.
10. Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness.
11. Ragan, S. (2014, July 16). No money, no problem: Building a security awareness program on a shoestring budget. Retrieved November 05, 2017, from https://www.csoonline.com/article/2454634/security-leadership/no-money-no-problem-security-awareness-program-on-a-shoestring-budget.html
12. Navarro, L. (2007). Train employees-your best defense-for security awareness. *SC Magazine Online*.
13. Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862.
14. Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352-357.
15. Communications and Information Technology Commission and Computer Emergency Response Team, Saudi Arabia CITC /-SA – (CITC),

Information Security Policies and Procedures Development framework Framework for Government Agencies. Retrieved on 20th Jan 2017 http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/OtherRegulatoryDocuments/Documents/CITC_Information_Security_Policies_and_Procedures_Guide_En.pdf