# DEVELOPING INFORMATION SECURITY MULTIMEDIA TRAINING PROGRAM UNDER SECURITY ANALYST WORKBENCH

**Wajeb Gharibi, Hassan Ktaiman**
College of Computer Science & Information Systems, Jazan University, Jazan, KSA.
*gharibi@jazanu.edu.sa, hktiaman@jazanu.edu.sa*

***ABSTRACT**: In this paper, we propose our methodology of enhancing the awareness of general cyber-threats for our students in Jazan University where we intend to meet the needs of our students to guide and teach them a solid background of the basic knowledge of potential cyber threats, different types of security issues with anti-defense tools and techniques. We believe that technology alone is not enough to provide adequate information security and it needs personal awareness and responsibility which are considered the most important to any information security program.*

**Keywords**: Information security, awareness, training and awareness program.

## INTRODUCTION:

Information is the most important and valuable asset of organizations, but security breaches of this information are critical issues that can lead to loss of integrity, availability, and confidentiality beside disruption of critical services. With the present of general public disclosure laws, the security breaches of personal or private information damages the firms' reputation and causes legislative sanctions. This influence of security violation is very clear, but mostly estimating this impact is not easy. So security awareness training is very important to all staff members in universities and all types of organizations. It gives the knowledge of potential threats and the ability to anticipate what types of security issues and incidents faculty, staff, and students may face in their day-to-day functions. Technology itself cannot provide sufficient adequate information security. Security awareness training and personal responsibility are very important critical issues to the success of any information security program. Generally, Information Security encompasses three elements which are a) Confidentiality that insures the disclosing of information, B) Integrity which ensures the accuracy and completeness of information and processing methods, C) Availability that ensures the accessibility of information.

Lately, increased breaches in all domains of information security; personal interests, national and social stability and economics, have made a wake-up call for the global information security. In answer to that breaches, most countries such as USA, Canada and UK and many others start improving the awareness and curriculum education program of information security and different cyber threats [11].

In our opinion, information security training is required for all individuals with security access to sensitive or confidential systems, each individual must complete such training and supervisors must also certify and track the completion of security awareness training program for each student and staff member or user in the institution/organization.

We intend in our suggested security training program to develop enterprise security architecture at conceptual, logical, functional, and physical levels, which can manage risks and prevent users of being victims to hackers and other potential cyber threats. It will be defined in business terms to help not only our students but also nontechnical stakeholders and able to provide security-related feedback to business owners and stakeholders.

We believe that human factor is the most important object in information systems and information security. From an educational point of view, information security training programs need solid theoretical and practical basics of information security concepts, so we developed our proposed training program with a very strong basic of theoretical and as well practical scientific foundation of information security.

## 1. LITERATURE REVIEW:

There are plenty of papers in literature tackle the problem of information security. Among them, paper [1] which measures the influence of security violation on an organization within the market. Security breaches are studied as well as the reports and news articles corresponding to those breaches to determine when the event was disclosed publicly in order to address the main issues on the stock market caused by those security breaches. Authors of [2] propose an innovative approach that focuses on two issues. First, the Policy model that takes into account the responsibility of stakeholders. Second, the policy engineering method that takes care of business process while using the principles of requirement engineering. In thesis [3] Developing a Risk Management System for Information Systems Security Incidents, author introduced that Internet has made very big peaks for business and customers by reducing cost, time and improving availability but it brought with it a wide range of risks and concerns especially in the field of business, private and sensitive information. It provides a managements perspective on the main issues challenging IT managers and CIOs including information security and its techniques. In addition, it created some classification of threats for its evaluation supported by examples.

The International Series on [4] are aimed to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas.

Chapter 5 in [5] describes reverse engineering as a technique to the find the design of software from its binary. Academics, researchers, and security professionals use reverse engineering to learn software design for a variety of purposes not limited to writing an anti-privacy wrapper software, copyright and patent, malware analysis, malware creation, data recovery, and discovery of undocumented APS. It discusses the anti-reversing techniques that include the

concepts of disassembly, virtual machine detection, and anti-debugging. [5] Provides the organizations with recent cyber threats. Reference [6] covers various exposures that companies face regarding technology, its vulnerabilities, and the new perils that cause information risks with classifying the type and degree of the risk. Moreover, the paper examines the processes and controls that companies take to minimize the risks and their affects. The paper does not only addresses the techniques used to react, respond, and remediate when unwanted event occurs, but also covers the forms of available insurance to help alleviate the financial pain associated with these unwanted events.

Author of Paper [7] tried to develop training information systems security program for public and governmental organizations in Turkey.

In fact, information security can be managed through three separate mechanisms: organizational factors, behavioral factors and training. Each of these elements impact differently on information security and comprehensive solutions include combinations of all three [8, 11, 12].

E-Laboratory for students training of security concepts in suggested in [9]. It presents the design and implementation of the e-laboratory that covers most of important aspects of information and network security. The e-lab can also be used to detect the security breaches of the system and even the development of information and network security.

Paper [10] conducted a survey of current situation of information system literacy (ISL) education of undergraduates of four Chinese universities, and suggested an information security literacy training.

In papers [13-16], we study the cyber threats in social networking websites, propose the phishing attack stages and types and discuss the different cyber threats and their protection technologies.

We concluded our papers with some important recommendations for preventing phishing and information security breaching. We integrated our studying about the most significant malicious software in paper [17].

## 2. DEVELOPING AWARENESS PROGRAM

We start our awareness program from the basic information about information security by establishing the related terms in a very simple understandable way to our students. We give the definition of computer, explain computer diagram and its two different parts hardware and software in details. Then we handle the terms internet and world wide web and the way of information transmission within the internet. After that, we define computer security tools and methods designed to protected data from different attackers and threats where network security strives to protect data while transmission from one location to another over the internet. In our training, we give basic information of malicious software and threats accompanied by the antitechniques. We summarize them as followings:

Malicious software can be divided into two groups" a) independed (the bad ware does not need host program, such as , worm and zombie), b) Dependent (need host program) such as trapdoors, logic bombs, trojan horse and viruses.

Viruses: small malicious codes hided themselves on the computer (such as Love Bug and Code Red) and they can delete information and ruin documents and even can format and destroy the hard disk. Viruses can replicate and spread to other computers by sending a copy of themselves by email on the network. There are so many types of viruses and can be classified according to the method they attack, such as boot sector viruses, memory resident viruses, stealth, polymorphic and metamorphic viruses and many others.

Trojan horses: appear as legitimate programs with hidden-side effects. Usually allow hackers to indirectly gain access to their target and often used to install backdoor or to destroy data.

Worms: self-replicating but not infecting program and typically spread over the network and widely used to create zombie PC's for further attacks, especially DoS. ( Blaster , Sasser ).

Rootkits: low level malicious programs embedded in the operating system itself and very difficult to be detected and deleted.

Adware/Spyware: are designed to gather information about the potential victim user and his habit, purchasing and web browsing intended to marketing purposes or others they may be harmed operations. Email attacks: can be done by phishing, malicious attachments, hoaxes, spasm and scams. Here, for our best practice, we should not open any suspicious attachment or follow any link or even attempt to "unsubscribe".

Social Engineering Techniques: Social engineering-the act of social hacking is considered one of the most effective methods of stealing confidential information and data of organizations. Generally, thief's go through the many tactics and uses very tricky ways of manipulation to steal money/information from victims such as: Pretexting – creating boke scenarios, Phishing – fraudulently obtaining private information, Fake websites/ Fake pop-up and Baiting. Generally, people are more vulnerable than computers, i.e. you are the weakest ring in computer security series! Sometimes small piece of information could compromise what you are protecting. In fact, an active security awareness training program can greatly reduce computer risks which cannot be addressed through establishing new software of hardware.

Security awareness training for our university students is a critical issue of our cyber security program. We provide a high-level view of the latest advanced strategies that handle cyber threads and address new vulnerabilities risks in which results in helping our students in Jazan University. They can attend our training program and get knowledge about information security, social engineering and anti-phishing risks. Here, we mention some programs for cyber security training in Saudi Arabia, (Dammam, Jeddah, Mecca, Medina, and Riyadh) where the cost is SAR 17495 for 2 days training on the foundation of information security, pretends covering the topics: business continuality, encryption, handling company information, handling payment cards, hackers, crackers and on-line crime, identity theft, malicious software, mobile phone security, passwords, phishing and Wi-Fi security [18]. We believe that determined time is not enough to cover the suggested program and the cost is very expensive. We concentrate on the four critical issues of information security which are confidentiality (ensuring the disclosed of information), integrity (ensuring the accuracy

and completeness of information and processing methods, availability (ensuring the accessibility of data) and transparency (ensures the quality of information). See Diagram 1 which summarizes our policy:

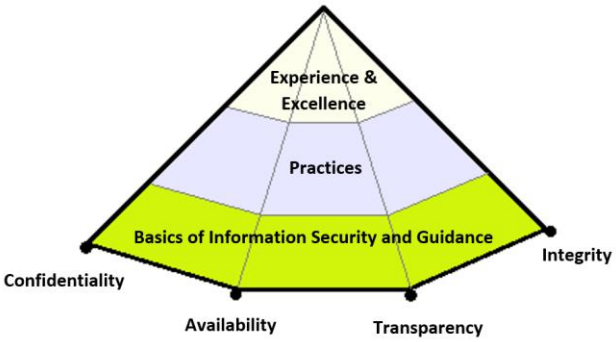


**Figure1. The Critical Issues of Information Security**

Our Awareness program is designed for our students at Jazan University to guide them for taking future decisions related the information of security issues. Our goal is to stair up the following diagram (see Diagram No.2):

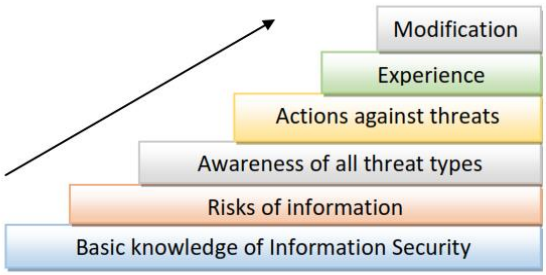


**Figure2. Training Program of Awareness of Information Technology**

The diagram describes the important steps of our awareness training, which starts from the first level; Basic knowledge of information security where we concentrate more on this phase to empower the basic knowledge of our students of information security. Then we explain the different risks of information. After that comes the awareness of all threats types with the suitable actions that should be taken against them. Hence, our students will be given suitable time training to get good experience of information security tools and techniques. Finally, we continuously work over the modification of our training program in the sense of new cyber threats and appropriate defense techniques. We suggest some recommended techniques for our students to help them get away of any type of cyber attacks:

- Authentication is very important and the 1-st line of defense against all types of threats, so we should have very strong secret password to enter the system which we want to access.
- Updating anti-viruses with active firewall all the time
- Rejecting and not downloading any types of documents from any suspected email or sites.
- Inform the IT center immediately in case of in case of suspect that you have fallen in a trap and you are a victim of fraud, theft or hacking attempt.

## 3. CONCLUSION AND FUTURE WORK

In this paper, we introduced the importance of information security and proposed a description of training program to our students in Jazan University. The suggested program concentrate on establishing solid knowledge-base of information security, its terms and terminologies, cyber threats and recommended antitechnologies to prevent breaches and protect information. Our future work will stress on the feedback of our training to enhance our program with new threats and tools and getting it up to date.

## ACKNOWLEDEMENT

We would like to thank the Deanship of Scientific Research of Jazan University for supporting this paper under the Grant No.1298/S2/36.

## REFERENCES

[1] Sanjay Goel, Christopher Brown, Hany Shawky, “Measuring the Impact of Security Breaches on Stock Valuations of Firms”, Proceeding of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas.

[2] Christophe Feltus, “Preiminary Literature Review of Policy Engineering Methods Toward Responsibility Concept”, Information and Communication Technologies: From Theory to Applications 3rd International Conference ICTTA, Damascus, 2008.

[3] Fariborz Farahmand , “Developing a Risk Management System for Information System Security Incidents”, College of Computing, Georgia Institute of Technology, 2004.

[4] Sushil Jajodia, “Identifying Malicious code through reverse Engineering”, Springer International Series on ADVANCES IN INFORMATION SECURITY, ISSN: 1568-2633

[5] The Notorious Nine: Cloud Computing Top Threats in 2013

[6] John Wurzler, Information Risks & Risk Management, 2014

[7] ASlm Genger G6kce, "The Public Information Systems Security Program", International Conference on Information Society (i-Society 2012).

[8] Nesren Waly, Rana Tassabehji and Mumtaz Kamala, "Improving Organizational Information Security Management: The Impact of Training and Awareness", 2012 IEEE 14th International Conference on High Performance Computing and Communications.

[9] Siddeeq Y. Ameen, Ibraim M. Ahmed, "Design and Implementation of E-Laboratory for Information Security Training", 2013 Fourth International Conference on e-Learning.

[10] NING Yuwen GAO Donghuai SHEN Xiajuan, CAI Hua, "Designing A Training Program For Information Security Literacy Of Undergraduates Based On Ubiquitous Learning", 2014 International Conference of Educational Innovation through Technology.

[11] Eric Amankwa, Marianne Loock, Elmarie Kritzinger, "A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definition", The 9th International Conference for Internet Technology and

Secured Transactions (ICITST-2014).

[12] Nesren Waly, Rana Tassabehji and Mumtaz Kamala, "Improving Organisational Information Security Management: The Impact of Training and Awarenes", 2012 IEEE 14th International Conference on High Performance Computing and Communications.

[13] Wajeb Gharibi, Maha Shaabi, "Cyber Threats in Social Networking Websites", International Journal of Distributed and Parallel Systems (IJDPS), Vol. 3, No. 1, January 2012.

[14] Wajeb Gharibi, "Some Recommended Protection Technologies for Cyber Crime Based on Social Engineering Techniques – Phishing," Journal of Communication and Computer, Vol. 8, No. 7, 2011.

[15] Wajeb Gharibi, Abdulrahman Mirza, "Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies," International Journal of Computer Science Issues (IJCSI), Vol. 8, Issue 1, 2011.

[16] Wajeb Gharibi, Abdulrahman Mirza, "Security Risks and Modern Cyber Security Technologies for Corporate Networks", International Journal of Computer Science and Information Security (IJCSIS), Vol. 9, No. 1, 2011.

[17] Gharibi W., "Studying and Classification of the Most Significant Malicious Software", Journal of Communication and Computer, Vol. 8, No. 1, 2011.

[18] https://www.theknowledgeacademy.com