https://doi.org/10.48009/1_iis_2010_402-409

A FRAMEWORK FOR INFORMATION SECURITY AWARENESS PROGRAMS

Carlos M. Figueroa Domínguez, Universidad del Turabo, cmfigue@yahoo.com
Mysore Ramaswamy, Southern University, mysore@acm.org
Eulalia Márquez Martinez, Universidad del Turabo, emarquez@suagm.edu
Mariano García Cleal, Universidad del Turabo, mgarcia@suagm.edu

ABSTRACT

The importance of information security cannot be overemphasized in today's networked corporate world. A major component of reducing the risk of security breach in information assets is by implementing an effective security awareness program in organizations. Empirical data for this research is based on a study of two highly regulated industries – Banking and Insurance - in Puerto Rico Metropolitan Area. In this paper, we look into the various factors that go into the designing an effective security awareness program and how such a program can help companies reduce the risk of security breach. Management support is very important for the success of the program. We analyze methods for building a successful security awareness program and present a set of recommendations for strengthening the program.

Keywords: Information Security, Risk Reduction, Security Awareness, Security Controls, Social Engineering.

INTRODUCTION

The importance of information security cannot be overemphasized in today's networked corporate world. A major component of reducing the risk of security breach in information assets is by implementing an effective security awareness program in organizations.

One of the major problems enterprises face today regarding information security is due to the lack of importance given to the implementation of security awareness programs in their facilities. People who are unaware of the fact that they are placing company's privileged information at high risk commit security breaches. Peltier [17] stated that an information security protocol could not be effective without implementing an information security awareness program and provide training for employees to show them how to follow policies, procedures, and tools.

One of the challenges to information protection is the need to implement and/or improve different technological controls and develop policies, procedures, and guidelines to maintain the confidentiality, integrity, and availability of information and minimize the risk of leaking it to the wrong hands. Some companies devote a lot of time and effort establishing technical controls to protect information resulting in increments in the operational budget for information security, but leaving the final user unaware of security topics that can put all the technology investment to a crawl. Although technological methods of protecting information may be effective in their respective ways, many losses are not caused by a lack of technology or faulty technology but rather by users of technology and faulty human behavior [10, 13, 15].

It is sometimes forgotten that computers and technology are merely tools, and that it is the human being that is using, configuring, installing, implementing, and abusing these tools [9]. Technical controls are essential to information protection but people can disclose and/or destroy information using different technologies available today thus resulting in enterprises not complying with regulations, and losing its reputation. While many technical means are used to secure corporate systems, individual employees remain the last line – and frequently the weakest link – in organizational defense [2]. The security of any system is best seen as a chain of components, only as strong as the least secure one. Confidence or assurance is also a chain, as strong as the least trusted link. In each case the weakest component, be it computer or human, limits the effectiveness of all others [3].

In a survey conducted in 2004 by Ernst & Young [6], respondents named lack of security awareness by users as the top obstacle to effective information security. According to the 2006 Computer Security Institute/FBI (San Francisco Federal Bureau of Investigation) Computer Crime and Security Survey [8], virus attacks were reported to be the source of the greatest financial losses, insider abuse followed by unauthorized access, losses related to laptops or mobile hardware, and theft of proprietary information

collectively accounting for approximately 75% of the losses.

The purpose of this paper is to present the benefits of implementing security awareness programs for information protection in organizations, and using those programs as vital complements to technical tools. This research is based on empirical data gathered in Puerto Rico Metropolitan Area from two different sectors: banking industry and insurance industry. There has been little or no research literature about security awareness programs in Puerto Rico Metropolitan Area especially in banking and insurance industries. The available literature, which is in general terms, pertains to other countries or geographical areas. The objective of this research is to examine the status of security awareness of users in terms of what is done, how it is being done, and what they are doing to assure the confidentiality, integrity, and availability of information, and minimize the risk of security breaches. These are topics hardly covered in current literature. The rest of this paper is organized as follows. The next section describes the nature of security awareness. The results of the survey conducted for this research are analyzed in Section 3. The last section presents recommendations to reduce the risk of information breaches in organizations.

THE NATURE OF SECURITY AWARENESS

Federal Standard 1037C (1997) defines Information Security as: "The protection of information against unauthorized disclosure, transfer, modification, or destruction whether accidental or intentional." Information Security includes many subjects, from high level principles and policy right down to the very detailed calculations in encryption algorithms [7].

Risk can be defined as: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets," and vulnerability can be defined as: "A weakness of an asset or group of assets which can be exploited by a threat" [11].

The Chief Information Security Officer (CISO) may have delegated responsibility for establishing and managing many of the technical solutions that contribute to information security, but overall governance and assurance of the security's effectiveness must reside with business management [19]. Related to the procedural aspects, one of the responsibilities of CISO is to inform company employees of the critical importance of information security; this awareness needs to be related to risk, policies, standards, procedures, and guidelines in a way that are easy to understand and follow. When the policies need to be communicated, "Security is an integral part of the entire business process and must use the words and objectives of the business units to be successful" [17].

According to Wulgaert [20], creating awareness involves more than pushing or communicating information to people; it requires understanding, learning, acquiring skills, and using the obtained knowledge of which the latter is critical to the success of the security awareness program. The success of the program depends on the change in peoples' behavior. But often people do not change their behavior. Insider abuse, laptop theft, viruses, and unauthorized access are among the most common incidents companies have faced in the last five years. When individuals choose to disregard security policies and procedures meant to protect the organization, they leave the organization at risk [2].

Security awareness programs need to stay up-to-date with new methods by observing people who like to obtain company information via technical methods like spyware or non-technical methods like social engineering. Often, social engineers try to gain a person's trust because people are more likely to give information to a person they trust. Social engineering derives much of its success to get the necessary information for an attack by preying on the helpful, trusting nature of most people or individuals who display signs of being susceptible to this psychological attack [9].

The learning curve in information security field consists of three key elements [17]. The first is awareness used to stimulate, motivate, and remind the audience the expectation from them. The second is training, the process of teaching skills or manage required tools. The third is education, the required time in depth dedicated to support the tools.

According to information security professionals, the two critical issues are the senior management support for enforcing information security and the availability of security awareness training for users [12]. The key to show improvement and value for information security is to translate it into business terms [16]. The effectiveness of information security program is based on availability of information resources and the processing of them when authorized users need them [17]. To have a successful information security program, it must be lead by confidentiality, integrity, and availability of information.

Peltier [17] proposed that enterprises need to show the audience five key elements. Those elements include first, the process to communicate the message to user community to enforce the concept of information security as an important part of business process. The second element is to identify the entity responsible for the information security program implementation. The third element is the ability to determine the importance of information and the criticality of applications, systems, and business processes. The fourth element is the business reason for the implementation of basic security concepts like separation of duties, need-to-know, minimal privilege. The fifth element is about management supporting the goals and objectives of information security program.

Desman [4] gives a series of ten tips to reach enterprise users. The first tip is show that information security is a matter of people, not technology. No matter how strong are the technical security devices, if policies, procedures, standards, and guides are not followed, user can open doors for security incidents. Second tip is to talk to your audience in their language. Communicating the same way to security administrator and clerks is not a good practice. Segmenting the audience is a good idea to start awareness. The third tip is to show documentation that users can see and react. Documentation, brochures, publications can help to show what is needed.

Fourth tip is to establish the purpose of the activity in a way that audience can also identify. Stick to a specific topic and do not confuse the users. Fifth tip is to handle the process with humor. Relax the audience to absorb the topic. Sixth tip is to create the purpose, support it, and finalize it. Summarize briefly the topic presented. Seventh tip is to convince audience that their behavior affects them. Highlight the advantages to the enterprise and the advantages to them.

Eighth tip is to maximize your strengths. Use the communication vehicles to the extent possible. Ninth tip is to formalize the training method. Present an organized structure and be consistent with the purpose so as to make user understand that it is a serious manner. Finally, adhere to a formalized schedule. It is recommended that when new threats arise, users get prompt communication that enables them to prevent security breaches.

SURVEY RESULTS

The purpose of this study was to investigate risk reduction by implementing security awareness program in Puerto Rico metropolitan area companies. The status of security awareness program, social engineering awareness, information security policies and compliance of those policies, auditing, and user perceptions in banking and insurance companies in Puerto Rico metropolitan area were examined. We observed the way security awareness was established in banking and insurance organizations and factors affecting or influencing effective information security throughout organizations. This research also examined the differences between various security awareness programs. The study covered all information stored in both, electronic, and physical form, in order to include all possible information, the company owns.

In this study, information regarding security awareness in organizations was gathered from the users. The objective was to correctly identify the status of security awareness in enterprises, policies regarding information security, user perceptions, compliance, and social engineering awareness. We also wanted to know whether all members of the organization had the same opportunity to participate in the security awareness programs. This study was not targeted to information systems personnel only but also to the users who handle information everyday to do their job. A formal contact with personnel from surveyed organizations was established to conduct the research. The meeting was meant to explain the purpose of the study which is twofold. First, the importance of improving the information security in their organizations was explained. Next, the confidentiality of the data obtained protecting the organization that answers the questionnaire, and protection of the participants letting them to answer the questionnaire anonymously without questions that help identify them was assured.

The results were used to compare to what extent the users in various organizations were aware of the security protocols. In addition, the results of this study will help in evaluating the techniques that are being used for user training on information security protection. This information will also be used to develop, improve, and implement various components of a security awareness programs in different businesses such as insurance companies and banks. By optimizing the efforts towards security awareness training, organizations can maximize the return on investments pertaining to information

security. Enterprises can evaluate the topics that need to emphasize of security awareness and can focus on the solutions they really need.

The study also took into consideration the risk an organization can face depending on user awareness of security. Based on the degree of information security awareness, the businesses received recommendations to improve the level of awareness and reduce the risk associated with managing information. The study also covered the security awareness from the perspective of normal users like secretaries, clerks, supervisors, managers and other non-IT Staff. IT Staff also were interviewed but they were not the main focus as in other studies. Some studies have examined motivational factors and attitudes affecting behavior and willingness to follow organizations mandates.

About half of the respondents perceived that security awareness fits their needs and/or their suggestions were considered. Frequently they read security policies and received training in security issues. They also stated that it was very important that they could easily access security policies. Management was very much involved in security awareness training and developing awareness of social engineering.

The common delivery methods for security awareness training were face to face training sessions 21.95%, e-mail messages 30.08%, and presentation by speakers and online training tied at 15.45%. The common topics covered in security awareness training were acceptable use policy 10.89%, confidentiality 10.00%, password protection 9.78%, computer security 8.67%, integrity of data/information 8.00%, specialized compliance (HIPAA, FERPA, GLBA) 7.56%, and identity theft 6.44%.

It was interesting to note that 87.27% of respondents follow security policy all the time but 24.59% share their password with someone. This is in spite of the fact password protection was selected as the second most common topic on security awareness training. 64.29% of respondents reported that social engineering awareness tests were conducted in their organization.

Regarding user perceptions, we need to highlight that participants reported that security awareness was an ongoing focus in their organizations; security awareness goals were clearly identified and communicated. On the other hand, people did not feel empowered to make decisions involving the security of information and technology, they did not feel that they were rewarded or recognized for good security behavior.

In an interview with companies, CISOs reported that security awareness programs were conducted for a period of five or more years, and they did receive support from top management for the program. They also reported that they only faced one major issue of information leakage by personnel in a five year period, and only faced two virus outbreaks in the same period of time. You can see the effectiveness of security awareness programs in the companies studied compared with the overall organization experiences.

RECOMMENDATIONS

Information is an important asset for companies and needs protection; one way to help protect this asset is to instill awareness in people who manage it in security topics. There is a need to encourage in different and new ways to diffuse the message through organizations. The effective communication of a security awareness program is essential and all users within the organization need to have the same knowledge regarding security awareness, policies, and procedures.

The information technology risk management framework is composed of policies, procedures, practice, and organizational structures. The framework also addresses people, process, and technology and encompasses the physical, technical, contractual, and procedural aspects of the organization. The purpose of this framework is to give organizations tools to implement security awareness programs and provide a different perspective to achieve risk reduction. The following framework helps in implementing security awareness programs in organizations.

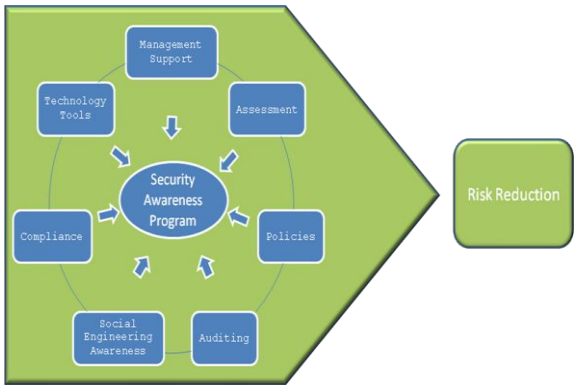

Figure 1. Framework for Implementing Security Awareness Programs

The different inputs like social engineering awareness, technology tools, and compliance are options available to initiate security awareness programs within organizations. The input from the framework can be used alone or can be interrelated with others.

The more input that enters the security awareness program, the better. Enterprises can implement social engineering awareness alone as a good start, but can combine with auditing, implementation of policies, and assessment for validation of user understanding of social engineering. Enterprises can also use technology tools for diffusion of the message.

One effective mechanism to enhance information security is through technology. Perform web based training sessions, and record the face-to-face sessions to post them on the intranet to facilitate the distribution to all organization members in a massive way. This can be convenient for participants who are unable to attend face-to-face sessions. These training sessions can be arranged at least once a year. The use of built-in computer technology like wallpapers and screensavers with security awareness message can help increase the scope of security awareness training. Examples are information security new topics that need to be incorporated frequently in the security awareness program, new threats, security breaches and methods to obtain company information needed to be integrated in the security awareness program. With the use of computer technology, addition of those new topics as an add-on using screensavers, e-mail messages, or other rapid diffusing technique can be established. This can help meanwhile a schedule for a new security campaign for face-to-face sessions or web sessions can be arranged.

As assessment is very important for a program continuous improvement, maturity, and growth, small quizzes to validate the understanding of security awareness training knowledge needs to be added at the end of each session. Those quizzes help also retrieve information on weak areas, user needs and enforce the security awareness program participation to people in organizations.

The security awareness program message needs to be repeated often, and the procedures to report security incidents needs to be clearly identified by the administration of the organizations. Guiding people to become aware of security topics is crucial, however equally important is to make employees be ready to identify and act responsibly when faced with security incidents.

Emphasize topics like password protection and communicate the consequences to account owners who give passwords to others, never remove this from security awareness programs and provide often reminders, at least once a month. Explain users that password protection is responsibility of the user and the disclosure of passwords help others to perform system activities with their accounts. The system activities can be harmful and the owner of the account can be prosecuted.

The main goal of delivering a security awareness program is to build a strong security culture throughout an organization. With risk management the potential cost or impact of a particular activity can be determined. Risk management provides rationale and justification for all information security activities.

Understanding of the organization threats, vulnerabilities and risk profile is required. Also there is a need to understand risk exposure and consequences of compromise and stay aware of risk management priorities based on potential consequences. Build a risk mitigation strategy that residual risk impact have acceptable consequences.

These challenges are due to the fact that there are different forms of threats, different level of users, new compliance requirements, costs associated with information protection, some indifference of executive management about information security, among others. The combination of these factors can increase risk significantly.

The relevance and criticality of information security today gives rise to the necessity for managing information risk in addition to the multitude of other risks with which organization is faced. For effective risk management a solid foundation performing a comprehensive risk assessment combined with a business impact analysis is needed.

There is a need to understand the nature and extent of risk to information resources and the possible impacts. For risk management to be accomplished a balance of risk exposure against mitigation costs to implement appropriate countermeasures and controls are needed.

Peter Bitterli [1] narrates the evolution of security management in a Swiss insurance company named Swiss Re. He describes that the company was found

wanting regarding information security and its transformation to a better information technology (IT) security strategy. Some of the changes pertaining IT security were applied to employees, contractors, and suppliers, all responsible for information security. With this new security policy, IT organization has to be broken into groups. The first group is the IT security committee; it provides group wide management direction in IT security and ensures that IT security is consistently addressed as a business issue.

The second group is the IT security office which develops and co-ordinates all aspects of IT security group wide. Activities include the development and implementation of group wide IT security policies and guidelines, awareness programs and training, support for IT security officers, and the handling of any IT security incidents affecting the organization as a whole.

The third group is IT security officers in divisions and major legal entities, security officers manage and co-ordinate IT security activities within their units. Activities include the assessment of risks, consulting and support relating to IT security measures and their implementation, heightening IT security awareness, managing training activities, handling IT security incidents, and organizing regular IT security status checks.

The strategy is composed of four concurrent security IT security initiatives. The first initiative is the High-risk consisting of high risk technical issues covering range of topics like secure access for e-customers, standardization and reduction of Internet access, encryption for remote access and hard disk on computers, hardening of network perimeter, and improvement of antivirus measures.

The second initiative is awareness and training, Swiss Re was focused on changing the behavior of people, they wanted the internalization of security behavior in all aspects related to work. The targets were managers, IT staff and all other users of IT. The campaign began with videos, brochures, articles, security web sites, pop-ups and so on. Another form of delivery is classroom-training. They report that 89% of the participants intended to adapt their behavior after the courses.

The third initiative is Monitoring, Intrusion Detection and Incident Management. The objective is to measure and verify the effectiveness of security controls. This was mainly handled by setting up intrusion detection systems and response management capability and performing security penetration tests as well as other security reviews of networks and platforms.

The fourth and last initiative is *Best Practice in All Other Areas;* they focus on BS7799/ISO27001 operational aspects. BS7799/ISO27001 is the code of practice for the management of information security. While compliance is not a legal obligation, it benefits businesses and is accepted as a good ‘handbook' for effective security policy. Distinct from other initiatives that consist of project clearly defined, this is a collection of numerous small and medium task and activities aimed at improving operational effectiveness. Improvement in documentation and control of IT internal process is emphasized. It is very important to talk about risk management, a process that has to ensure that the impact of threats exploiting vulnerabilities is within acceptable limits, and at an acceptable cost.

There are some vulnerabilities like defective software, improperly configured equipment, poor network design, uncontrolled or defective process, inadequate management, insufficient staff, lack of knowledge to support users, lack of security functionality, poor choice of passwords, untested technology, transmission of data unencrypted, lack of redundancy, poor management communications.

The IT management function needs to know risk concepts related to information security such as Service Level Agreement, Robustness and resilience, business continuity and disaster recovery, process reengineering, project management timelines, enterprise architectures, IT governance, data record management, IT policies, standards and procedures.

Technical concepts of security technology such as Application security measures, Physical security measures, Environmental controls, Logical access control, Network access control, Firewalls, Intrusion detection/prevention, Wireless security, Platform security, Encryption and PKI, Antivirus/malware, Spyware/adware, Antispam devices, Instant Messaging, Telecommunications and VoIP, also need to be understood.

Although technological methods of protecting information may be effective in their respective ways, many losses are not caused by a lack of technology or faulty technology but rather are caused by users of technology and faulty human behavior [10, 13, 15]. While many technical means are used to secure corporate systems, individual employees

remain the last line – and frequently the weakest link – in organizational defense [2].

Enterprises invest large amounts of money putting in place technological controls like firewalls, network access controls, e-mail filtering and more as countermeasures for security attacks. However, to achieve secure systems and data requires more than a focus on the technical issues; it also requires attention from management to design effective computer security policies and to motivate individual behavior to follow those policies [5, 14]. Humans represent a vital component in organizational information systems; their role in any security plan should not be underestimated.

REFERENCES

1. Bitterli, Peter (2005). IT Security Governance – A Low Start to High Maturity Level, *Information Systems Control Journal*, Vol. 1.

2. Boss, S. R. (2007). *Controls, Perceived Risk and Information Security Precautions: External and Internal Motivations for Security Behavior*. Ph.D. Dissertation, University of Pittsburgh, Pennsylvania.

3. Cormack, A. (2001). Do We Need a Security Culture? *VINE,31*(2), 8-10.

4. Desman, M.B. (2003). The Ten Commandments of Information Security Awareness Training. Information Systems Security, January/February, 39-44.

5. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67

6. Ernst & Young, (2004). *Global Information Security Survey 2004*. Retrieved on May 14, 2000, from http://www.ey.com/ global/ download.nsf/UK%20Survey_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf

7. Farahmand, F. (2004). Developing a Risk Management System for Information Systems Security Incidents. Georgia Institute of Tecnhology, Atlanta, Georgia. Retreived April 30, 2008, from ProQuest Digital Dissertations database. (UMI, No. 3199293).

8. Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). 2006 CSI/FBI Computer Crime and Security Survey. Computer Security Institute. Retrieved from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdfhttp://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

9. Hansche, S., Beri, J., & Hare, C. (2004). *Official (ISC)2 guide to CISSP Exam*. Boca Raton: Auerbach Publications.

10. Im, G., & Baskerville, R. (2005). A longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *The DATA BASE for Advances in Information Systems, 36*(4), 68-79.

11. ISO/IEC TR 13335-1, Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security, ISO/EIC, 1996.

12. Knapp, K.J., Marshall, T.E., Morrow, D.W., & Rainer, R.K. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help? Information Security and Risk Management, September/October, 51-58.

13. Mitnick, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis: Wiley Publishing, Inc.

14. National Cyber Security Alliance. (2005). Top Ten Cybersecurity Tips. Retrieved March 21, 2005, from http://www.staysafeonline.info/home-tips.html

15. Orchesky, C. (2003). Beyond Technology-The Human Factor in Business Systems. *Journal of Business Strategy, 24*(4), 43-47.

16. Patrick, J. (2006). Effective Operational Security Metrics. Information Systems Security, July/August, 10-17.

17. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Security Management Practices, May/June*, 37-49.

18. Rotvold, G. (2007). *Status of Security Awareness in Business Organizations and College of Business: An Analysis of Training and Education, Policies, and Social Engineering Testing*. Ph.D. Dissertation, University of North Dakota, North Dakota. (Publication, No. AAT 3277031).

19. Williams, P. (2007). Executive and Board Roles in Information Security. *Information Systems Control Journal, Volume VI.*

20. Wulgaert, T. (2005). Security Awareness – Best Practices to Serve Your Enterprise, Rolling Meadows. Information Systems Audit and Control Association. *Information Systems Control Journal, Volume III*.