The importance of a security, education, training and awareness program (November 2005)

Stephanie D. Hight, *CCNA*

***Abstract*— A Security Education, Training and Awareness (SETA) program can be defined as an educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness. A SETA program sets the security tone for the employees of an organization, especially if it is made part of the employee orientation. Awareness programs explain 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.**

***Index Terms*—Security Education, Training and Awareness Program, firewalls, Intrusion Detection Systems, Security Policy**

I. Introduction

END-USER computing has emerged as a vital component of the overall information resource of the organization. [1] This emergence has made its way not only into the information resource but also in the information security of an organization. The end-user has access to the most vital information a company has and either has the knowledge in how to circumvent the systems that have been put in place to protect the organizations information, or the lack of knowledge that is needed to protect this information, as well as the well-being of the organization's network itself. It is recognized that the more educated a person is, the better decisions they should make in business and life itself. The question needs to be asked why then is a vital part of the organization's security structure ignored and not given information about threats and vulnerabilities. The end-users are the ones who will see these threats and be taken advantage of much more frequently. This happens due to their lack of knowledge on what to look for which can lead to threats such as taking down the network or seriously divulging confidential personal information. The Information Security field has grown rapidly over the past years because of these threats, and the Information Security personnel seek to harden the network through firewalls, Intrusion Detection Systems and the like but frequently overlook the most prominent line of defense that an organization can have: the educated end-user. They can be and quite frequently are the last line of defense in a network, but if they don't have the tools necessary or the knowledge to defend their system, they are as ineffective as keeping a newly purchased firewall in the box. This paper will attempt to define the Security Education Training and Awareness (SETA) program, the benefits that it can bring to organizations who deploy them, and why it is important for a company to implement a security awareness program.

Manuscript received November 29, 2005.

Stephanie Hight is with the City of Raleigh, Raleigh, NC 27601 (e-mail: Stephanie.Hight@ci.raleigh.nc.us).

II. Defining a SETA Program

A Security Education, Training and Awareness (SETA) program can be defined as an educational program that is designed to reduce the number of security breaches that occur through a lack of employee security awareness [2]. Shanna Groves in "The Unlikely Heroes of Cyber Security" reviews the International Standards Organization 17799 in how to meet coverage requirements. Groves sees providing information security education and training as crucial to the organizations security management practices [3]. So crucial in fact that a Department of Defense directive has been in place for IT security training and certification since 1998 [4]. All federal government agencies are required to have a SETA program with mandatory participation and completion of the program from all employees [5]. This crucial program is noticeably optional in the private sector.

A SETA program sets the security tone for the employees of an organization, especially if it is made part of the employee orientation. It plainly lays out the security expectations that the employer has for the employee. This program cannot just review policy, part of it must consist of an explanation of the policies and why they exist. For example, if properly explained why an employee's password has to be a certain number of characters and consist of a level of complexity it is much easier for employees to accept this policy and not come up with creative ways of circumventing the system and therefore putting the network at more risk than existed before. If they could be shown how quickly a simple password can be cracked it makes more of an impact on the end-user in seeing the part they play in keeping the data and the network safe from intruders. In an interview with DJ Hess, CISSP, City of Raleigh Information Security Administrator, he was asked why it is good to explain the City's security

policy to the end-users and replied, "The need for your employees to assist you in the defense of your network is critical. While we can write policies, if we fail to communicate and gain acceptance of the policies they will be ineffective. By educating the end-users you may enlighten some to the defense in depth strategy that you are employing."

Awareness programs explain the employee's role in the area of Information Security. They show the users where they can play a vital 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 it encourages employees to care more about their work environment [5]. Awareness is the lowest level of the solution to information assurance [6]. The awareness part of the program gives the users the information to motivate them to learn more and be more attentive to details. Awareness should be the catalyst to the training part of the program which should consist of a more hands on approach to learning. One fundamental goal of training programs should be motivation of learners to move knowledge and skills from the short-term memory into long-term memory [6]. Awareness is the part of the training that puts the information into the short-term memory which should move that information into permanent application in the employee's everyday working environment. A SETA program shows the users how to put security in the forefront of their minds on a daily basis and what actions they should take to continually protect themselves as well as the organization's data and network. The aim of a security awareness effort is participation. A high motivated work force can be the best ally a security manager has.. The awareness program can show employees how security affects the company's future and protects them from physical harm or possible loss of employment by protecting assets [7]. The SETA program is meant to weave security into the fabric of the enterprise [8]. In focusing on the topics that end-users see everyday in their work lives, it incorporates security in every task that the user does, from locking the computer screen when they walk away from their desk, to being aware and reporting any strange activity that they see in regards to e-mail, files and personnel.

III. Benefits of Having A SETA Program

Having a work force that is educated and more aware of security areas is like expanding the Information Security department into the whole company. It gives the security manager or Chief Information Security Officer (CISO) a broader base of brainpower in which they can tap if needed. Instead of a staff of 10 trying to secure the network and protect it against viruses and external threats, it has everyone in the organization looking out for the security interests of the company. This can create a "human firewall" that can be more powerful than properly configured firewalls and Intrusion Detection Systems. Technology alone cannot solve the problem of securing a network, the term "Human Firewall" refers to the idea that the people within an organization, if made aware and properly educated, will support Information Security efforts and form a layer of protection (much like a firewall) to prevent and deter threats to a company's critical information assets [9]. Hess states if an organization can make people aware of their surroundings, both physical and electronically, it can help the organization to defend against the known threats and uncover the hidden threats.

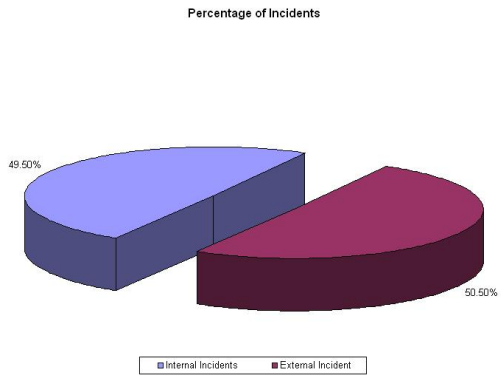

Figure 1 Source: CSI/FBI 2005 Computer Crime and Security Survey

Implementing a SETA program can be seen as a part of risk management. By integrating security and risk management into the organization and its ongoing processes, these important functions will become a way of doing business [10]. By having uneducated employees, a company is taking a very large risk in putting the security of the entire organization into the hands of a very few security professionals that cannot fully secure the information with only the help of technology. This risk can be extremely minimized through the implementation of a successful SETA program. Debra Donston in "A Healthy Security Attitude" quotes Donna Richmond, Aetna's InfoSec Architecture Manager as saying, "The major risk you're managing is the people you give access to; error and omission and people just rushing to get their jobs done." [11] With a training program in place, this reduces the risk of people making mistakes and causing problems which affect everyone in the organization. A painful reality for most organizations is that staff are often more responsible than intruders for data and information loss [10]. It is in fact a part of system access control. With the proper controls in place, an organization can restrict access to information and computer areas and educate the users who have legitimate access to this information, the data owners, in how to handle, process and transmit this data in a secure manner that does not compromise the security of an organizations most valuable asset, it's data.

IV. Why a SETA Program is Needed

It can be ignorance, lack or training or naiveté that causes employees to open a gateway in the organizations network [12]. The risk of employee misuse can be something that ends up affecting an organizations bottom line. The 10th Annual

CSI/FBI Computer Crime and Security Survey reports that Insider Net Abuse cost the 639 companies surveyed $6,856,450.00, while System Penetrations cost the companies $841,400.00 [13]. Viruses still lead the losses with $42,787,767.00 [13], and even though they are the most public of IT security breaches, the majority of end-users still have very little knowledge about viruses such as how they work and where they come from [12]. This lack of understanding becomes a greater risk with the fact that virus and worm writers are coming up with more creative ways to appeal to the user and find its way into not only the inbox but also the network itself. These viruses, worms and Trojans rely upon the ignorance of users to properly function and infect systems [14]. It can be depressing and devastating to the Information Security staff as to how effective the simple tactics of the social engineering of viruses can be employed to fool the end-user.

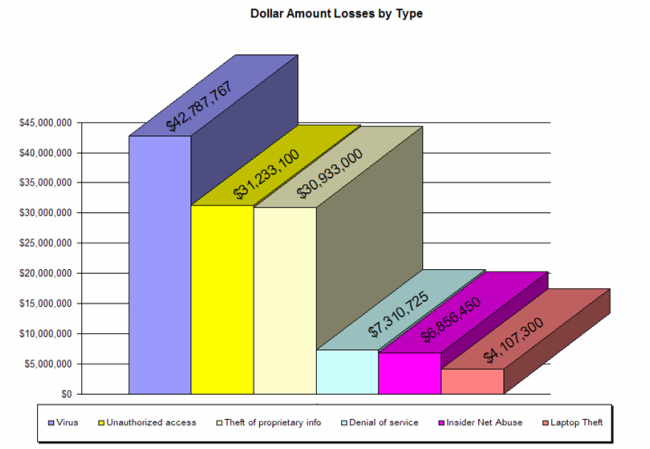

Figure 2 Source: CSI/FBI 2005 Computer Crime and Security Survey

Technology is both a friend and a foe to Information Security. With the prevalence of laptops, PDA's, Blackberries and other portable devices that connect to the network, all of which the majority of end-users are using on a daily basis, only opens more opportunities for external threats to make their way into the organization. These portable devices are small and often misplaced and lost, and with nearly 60 percent of the individuals using these devices not having in place any type of password protection or encryption, it only makes confidential information and access to the internal network easier to come by [12]. Morgan Stanley faced a potentially devastating problem when a Blackberry was put on eBay and sold for $15.50 by a former vice president with over 1,000 contacts and detailed loan terms, possible mergers and the personal information of the VP. This situation unfortunately is only one of many that have surfaced because employees have not been properly educated and shown why to store confidential information on these devices only when necessary and to employ vital tools such as encryption and password protection to keep confidential information confidential.

This situation can also be avoided by the properly written security policy outlining the guidelines that have to be followed with any device that is connected to the network, but a security policy can only be effective if staff, know, understand and accept the necessary precautions [15]. Policy has to be given out and explained fully in order for an organization to show that it has done its due diligence in trying to educate its end-users. It is not enough that a policy simply exist, but that policy must be disseminated throughout the organization to all employees. Employees need to have seen and understood the security policy of the company in order to know the adverse implications of not following and supporting the policy. Without a proper explanation, an employee can use ignorance of the policy as an excuse of not complying, thus tying the hands of the company if multiple infractions have occurred. This dissemination of the policy can and quite frequently is worked into the security education program. It gives the security personnel a chance to explain why these policies are in effect and how they protect not only the information of the organization, but the employees themselves and what the repercussions are of not following the policies.

Informed employees help assist in protecting assets and also themselves and their families from cyber crime and identity theft [14]. Employees who telecommute and use their personal computers to connect to the company's network must be educated and shown what the standards of the company are for desktops. Virus protection and personal firewalls are a necessity in this situation, but cannot be relied on as a guarantee of safety. An employee's child may have downloaded a Trojan posing as a game to that same computer and unknowingly, the employee has opened a window into the organizations network as well as their personal information that is kept on that computer. While an emphasis has been placed on securing the desktop operating systems and installing personal desktop firewalls, the weak link can quickly shift from the desktop operating systems to the operators themselves. Employees should be shown how it can benefit themselves as much as the organization they work for if they follow the written policies that are in place. It protects their confidential personal information that may be stored on the company's network or their personal computer from getting into the wrong hands and having years of problems in getting their credit or identity restored.

For some time it has been widely recognized that security is as much a people problem as it is a technical one, technical countermeasures are ineffectual if not supported by well informed end-users who are trained appropriately [6]. Technology alone cannot solve a problem that is controlled by individuals. The response to the problem must be a combination of technical and management. Top management must take an active approach to the security of their organization by supporting and following the policy themselves. Nothing can undermine a security education and awareness effort faster than lack of support from the management of an organization. If employees see their

superiors not taking the security of the company seriously then they have no reason to get involved and take an active role themselves. The support of management is critical to not only the security education program but the security policy itself. If part of the security management is not supported by not only management, but the employees themselves, the whole security program of an organization will fail. A SETA program should motivate users from the top of the company all the way to the bottom to get involved in the security of the organization. This motivation can be increased if the organization sets up an internal security certification program, whereby the employees are given a company security certification upon completion of the security education program much like Information Technology professionals acquire certifications. This company certification can bring recognition to non-IT employees who are actively involved in helping to secure the information of the organization. Motivation can also be achieved through a reward program. For example, if the company goes a designated amount of time without a security incident, such as no virus infections, all employees get an extra vacation day in the next year [16]. Although this may be difficult to achieve, the message that security awareness is important to management will definitely be achieved and be something that all employees strive to reach with an overall improved employee attitude toward the security policy. Hess has seen an improved attitude in the City of Raleigh employees when discussing threats such as phishing e-mails. In a SETA presentation to approximately 40 people Hess was explaining not only what the City IT personnel were doing to protect the employees, but what the employees themselves could do to help. The discussion ended with clapping and words of "finally!" from some of the attendees. "Obviously there was some history of inaction. Through the use of education and communication (being aware of your surroundings) we work together instead of just being those guys in IT. You can never over communicate."

Failure of a single component, such as a firewall or an end-user, may adversely affect the integrity, confidentiality, and availability of many or all critical systems on the network [6]. In the same way that technical failures or mistakes can be avoided with the proper technical training, end-user misuse or mistakes can be avoided with a well laid out awareness program. According to the CSI/FBI Computer Crime and Security Survey companies are increasingly taking into account the importance of a security education, training and awareness program. The companies surveyed rated the importance of a SETA program to different areas of security. The top four categories that were seen as the most important were: security policy (70 percent), security management (70 percent), access control systems (64 percent) and network security (63 percent). Even though these companies realized the importance of a SETA program in all areas of security, when asked if they thought their company was investing enough into an education program, all respondents, except the high-tech sector and the federal government, felt that not enough was being invested into security awareness. It seems that even though companies realize the positive effects that can take place when an awareness program has been implemented, it still has not resulted in an increased investment into this program.

V. Conclusion

Albert Einstein was quoted as saying "Problems cannot be solved with the same level of awareness that created them." The problem of end-user mistakes cannot be solved by adding more technology; it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management. This partnership can result in a well laid out security, education, training and awareness program; the level of awareness must be increased to achieve a well-rounded security management process. The benefit of an educated general business community is limitless. It can give the Information Security personnel extra eyes and ears that can discover and plug hidden threats that could not be done through the use of technology. Without the help of the end-users, an Information Security staff can feel as though they are fighting a loosing battle. The three fundamental countermeasures for defending information and data are technology, operations and awareness, training and education. [6] The failure of any one of these measures can result in a total failure of securing an organization's valuable assets. Security has and will continue to hold the attention of national and international audiences but through the use of a SETA program it can capture the attention of an organization's first and last line of defense- its end-users.

References

[1] Allison W. Harrison, R. Kelly Rainer Jr., "The Influence of Individual Differences on Skill in End-User Computing," *Journal of Management Information Systems*, vol. 9, Summer 1992, pp. 93-111.

[2] Michael E. Whitman, Herbert J. Mattord, *Management of Information Security.* Canada: Thomson Course Technology, 2004, p. 532.

[3] Shanna Groves., "The Unlikely HEROES of Cyber Security," *Information Management Journal*, vol. 37, no. 3, May/June 2003, pp. 34-40.

[4] "DoD Info Security Training and Certification Program Could Affect up to 100,000 IT Pros," *Lifelong Learning Market Report,* vol. 9, no. 24 December 2004, pp. 1-4.

[5] Michael E. Whitman, Herbert J. Mattord, "Making users mindful of IT security; awareness training is vital to keeping the idea of IT security uppermost in employees' minds," *Security Management*, vol. 48, no. 11, November 2004, pp. 32-34.

[6] Corey D. Schou, Kenneth J. Trimmer, "Information assurance and security," *Journal of Organizational and End User Computing*, vol. 16, no. 3, July-September 2004.

[7] Michael J. Witkowski, "Extra eyes and ears," *Security Management*, vol. 36, no. 4, April 1992, pp. 42-46.

[8] Jim Tiller, "Taming the New Wild West," *Information Systems Security*, vol. 14, no. 2, May/June 2005, pp. 2-5.

[9] Steve Kahan, "Information Security: On the Cusp of a Management Evolution," in *Management of Information Security.* Canada: Thomson Course Technology, 2004, p. 18-19

[10] Arthur C. McAdams, "Security and risk management: a fundamental business issue: all organizations must focus on the management issues of security, including organizational structures, skill sets, processes, and

methodologies for managing security and risk management," *Information Management Journal*, vol. 38, no. 4, July-August 2004, pp. 36-42.

[11] Debra Donston, "A Healthy Security Attitude," in *eWeek.*, vol. 18, no. 23, June 2001.

[12] Jared Wade, "The weak link in IT security: what good is cutting-edge network security if your own employees sabotage the system by misake?" *Risk Management*, vol. 51, no. 6, July 2004, pp. 32-36.

[13] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, Robert Richardson (2005). CIS/FBI Computer Crime and Security Survey (10th Annual). Available: www.gocsi.com

[14] Richard Starnes, "Staff education is vital to effective information security; Create a security culture," in *Computer Weekly.*, p. 36.

[15] S.M. Furnell, M. Gennatou, P.S. Dowland, "A prototype tool for information security awareness and training," *Logistics Information Management*, vol. 15, no. 5/6, 2002, pp.352-357.

[16] Mark Hall, "Secure the people," in *Computerworld*, March 21, 2005, p. 50.