Global Information Assurance Certification Paper

Irene Long

SANS Security Essentials GSEC Practical Assignment, Version 1.2f (8/13/01)

Title: Management, The Missing Link?
November 12, 2001

Employees have frequently been cited as being the weakest link in information security. The primary defense has been to use security awareness programs to get the message out. It is reasoned that employees cannot be expected to follow security policies if they are not aware of security threats and what is expected of them. However, more emphasis needs to be placed on management participation in security awareness. This practical will discuss management's role and offers suggestion on how management can actively support the awareness program by using a personnel security perspective.

An information security program is the collection of security policies, standards, procedures, and guidelines that protect the availability, confidentiality, and integrity of an organization's information assets including data and systems. According to Tom Peltier, the goal of the information security program is to meet the organization's business objectives, the organizational needs, and to reduce losses associated with the disclosure, modification, destruction and or denial of service. The key elements of a security program are to assign responsibility for the program, classify information assets according to the organizations values, implement the security concept of separation of duties into business processes and implement a security awareness program.[1]

A security awareness program is part of the overall information security program. It reinforces the information security program by promoting the message of how security supports the organization's goals and business objectives. A security awareness program is used to educate the user on the value of the organization's information assets, awareness of security threats and user responsibility to the protection of those assets. Without awareness and understanding, the user/employee poses a risk to information systems.

In order for the security program to be successful, employee involvement is necessary because their activities directly affect the computing environment. When developing the awareness program, it is important to determine the goals of what is trying to be accomplished. However, the goal should not be to simply raise awareness, train and educate but to ensure that real behavior change has occurred.

In the article, "Making Security Awareness Happen", Susan Hansche makes an important distinction between awareness and training when she states, "…During an awareness campaign, the end user simply receives information. It is designed to reach a broad audience using various promotional techniques. In a training environment, the student is expected to be an active participant in the process of acquiring new insights, knowledge, and skills."[2]

The expectation that the user will be an active participant in the learning process is important idea to consider. To learn, the user must be aware and understand. However, to change user behavior, the users must practice and receive reinforcement and

[1] Peltier, p. 201
[2] Hansche

affirmation of their behavior. What mechanisms do we have in our organizations to ensure that learning has occurred? How do we reinforce the knowledge that is taught in awareness training? How does this translate into creating a culture of security?

The answers to these questions are through management and through the expansion of the goals of the security awareness program. A program objective that simply "raises user awareness" will have limited results. To reinforce active participation in the individual user, we must integrate management practices and personnel security into the awareness program.

As noted by William Malik of Gartner, "…Organizations need to understand that security is not primarily a technology issue. Security is a cultural issue, a governance issue. Good management can overcome bad technology, but I've never seen a case where good technology overcame bad management."[3]

It is easy to understand why information security is mistakenly taken to be a technology issue when we analyze the approach usually taken to address the problem. Solutions tend to center around the use of technology and products. We talk about security defenses in terms of anti-virus software, encryption, firewalls and intrusion detection systems. More emphasis needs to be placed on the people who use the systems and work in the environment. This not only includes end user/employees but especially management who is responsible for directing and controlling the work place.

Information security is a management issue that requires the support and leadership of management. Senior management has overall responsibility for information security.[4] They are responsible to ensure the establishment of sound and clearly defined security policies. Senior management must also support enforcement of the policies through disciplinary action. Policies that are not enforceable are meaningless.

Middle and line managers are closer to the employees and have daily opportunities to promote awareness and a security culture. Because managers are responsible for setting and communicating staff expectations, they are in the best position to reinforce desirable behavior through positive and negative feedback and through their own modeling of good security practices. In addition, managers must address security issues as they occur. If not enforced in a timely or equal manner, the employee will get the message that the policies and procedures are arbitrary and not important.

In order to gain management's cooperation and to get them to play an active role in the awareness program, it is necessary to get management's buy-in. In "Translating Security for Managers", Frank Prince offers advice on how to do this.[5] "[The security manager must] …demonstrate that they understand and agree with management's

[3] Malik
[4] U.S. Department of Commerce, NIST, p. 16
[5] Prince

larger organizational and fiscal objectives." In other words, security professionals must explain security issues in business terms that managers understand. For example, if a proposal is made to conduct pre-employment background checks, it must weigh the cost of the investigations to the value of the information assets being protected, the likelihood of a problem being caused by an insider, and the negative impact it may have on the business. Security professionals that are able to tie security with business objectives are more likely to succeed in gaining the management buy-in they need.

Managers are people too and are also motivated by personal incentives. A manager can be given a personal incentive by including the manager's security performance as part of his or her performance appraisal. Feedback would be given to upper management on the manager's support of meeting security objectives and performance to key controls. At a detailed level, this might also include the number of employee security incidents that occurred in their area and the manager's handling of the incidents or issues. In addition, the department's performance on security audits and the amount of security training attended by management and staff can also be considered.

Management's involvement in the awareness program is also supported by British Standard 7799 (BS 7799).[6] BS 7799 addresses best practices for information security management and is currently under consideration as an international standard as ISO 17799. The standard identifies controls needed to secure information management systems and emphasizes senior management's support and involvement in information security management.

BS 7799 has ten areas of detailed controls one of which involves personnel security. Personnel security involves security policies and controls that are applied to employees. BS 7799 divides personnel security into three areas of focus:

1. Controls to identify security responsibilities by job definitions
2. Security training and education of users
3. Response to incidents and malfunctions

In the article, "Computer Security Isn't Just Computers", Dev Zaborav, offers additional information on personnel security.[7] Zaborav explains that a secure computing environment involves physical security (security of the data center), informational security (security of the data), and personnel security (security awareness of data and system handlers). Personnel security looks at the whole working environment and how it relates to the people working in the environment.

This holistic approach is also echoed in the article, "Managing the Threat from Within" by Eric Shaw, Jerrold Post, and Kevin Ruby.[8] However, this article is more detailed and takes a specific stand on taking new approaches to the security awareness program.

[6] Price
[7] Zaborav
[8] Shaw, Post, Ruby

Because poor management practices in the reporting of incidents, employee screening, and termination procedures have left companies vulnerable, the authors encourage that a new approach be taken with IT security awareness programs through personnel security. They propose that organizations conduct an IT Personal Security Audit (PSA) to evaluate an organization's ability to detect and prevent the potential damage caused by insiders. The authors suggest thinking about the organization as a series of systems that employees travel through. The processes of hiring, training, evaluation, transfers, promotions and terminations are all considered personnel systems that would be reviewed for opportunities of management intervention and improvement.

Although the objective of the PSA is to detect "at risk" individuals, their approach is useful in identifying real examples on how managers and other business unit activities support security awareness through management practices. By reviewing personnel systems through a personnel security approach, a manager action list can be developed.

The following list is provided as a starting point and involves many areas of an organization such as business unit management, human resources, training, and possibly legal. It represents a list of real actions that managers can perform. The objective is to utilize management practices to incorporate security awareness into all areas that touch employees.

Interviewing and Hiring
- Include security questions in the interview
- Utilize pre-employment screening test
- Review resumes for missing information or indications of past problems
- Verify information provided on the application and resume
- Conduct background checks (especially in positions that carry a high level of responsibility or access to sensitive information)

Job Placement and Control
- Verify employee's skill to perform the job
- Clearly define security responsibilities in job descriptions
- Review positions for sensitivity to the information that is handled
- Match access levels needed to perform the job
- Review job responsibilities for separation of duties

Orientation and User Training
- Include security philosophy in new hire orientation
- Provide ethics training
- Have employees sign a document stating their understanding and acceptance of acceptable use and privacy policies (consider having them sign this annually)
- Provide training that is specific to job function and level within the organization

- Provide incident response training (define employee role and how to report incidents)

Performance Reviews/Coaching
- Address security issues as they come up
- Communicate and explain the reason behind policies
- Communicate consequences for violating the company's policies

Transfers, Promotions, and Terminations
- Promptly notify appropriate areas when terminating personnel
- Review access levels upon changes in employment status (transfers, promotions and terminations)
- Conduct exit interviews

As stated previously, the above list not only involves managers but other functional areas of a company. These areas will need to be approached and activities will need to be coordinated. To further assist managers in learning to incorporate these practices, specialized training in these specific areas is also recommended.

After all this effort, an organization may want to measure their success in creating a security culture. William Malik offers a three question test that will give an indication on how effective the organization has been in reaching its employees[9] The questions are:

1. If an employee witnesses a violation of policy by second employee, would the first employee know that an activity was wrong?

   If the employee fails to recognize that what they have witnessed is wrong, it demonstrates a lack of understanding of the company's position on such activity and lack of awareness of the policies.

2. Would the first employee report the incident?

   When employees fail to report incidents, it can be for a variety of reasons such as, the fear of negative repercussions (being labeled a tattle-tale or a trouble maker), they may hold the belief that it is someone else responsibility, or that management will not be receptive.

3. Would employee know who to report the issue to?

   Not knowing who to report the incident to is an indication of several problems. It is possible that the employee is not aware of the policies, or that there is not a clear definition of who is responsible or that there is not a clear escalation procedure.

[9] Malik

If the answers to any of these above questions is no, then the organization knows that the awareness program has not been effective in reaching its intended audience. An information security officer can assist with the organization's security policy, standards and recommended controls. The information security officer would also be responsible for the development and implementation of a security awareness program. However, the organization must look back to its management to communicate and reinforce the security message to its employees.

In conclusion, a security awareness program plays an important role in the overall security program. The main goal should not only be to educate users, but to change user behavior. The only effective way of accomplishing this is through management support and practice. Management reinforcement of the security message in all aspect of the employees' work experience and environment is key to the success of the awareness program.

Other SANS' practicals[10] have provided good information on the importance of the awareness program, topics to include, and methods of getting the message across. Unfortunately, there has been less focus on what managers can do and how managers contribute to creating a security culture.

The security awareness program requires everyone in the organization to be involved and it requires management leadership and participation to succeed.

[10] See list of SANS practicals

References:

1. Peltier, Tom. "Security Awareness Program." Information Security Management. Ed. Harold Tipton et al. 4th ed. Boca Raton: Auerbach, 1999. 197-212.

2. Hansche, Susan. "Making Security Awareness Happen." 17 July 2001. URL: http://www.techrepublic.com/article.jhtml?id=/docroot/article/r00520010717aue01.htm&page=2 (12 Oct. 2001).

3. Malik, Wiliam. "Does Your Company Culture Value Corporate Security?" Interview with Bob Artner. 9 October 2000. URL: http://www.techrepublic.com/article.jhtml?id=r00520001009ggp05.htm (12 Oct. 2001).

4. United States. Department of Commerce. National Institute of Standard and Technology, Technology Administration. An Introduction to Computer Security: The NIST Handbook." Special publication 800-12. URL: October 1995. URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (2 Nov. 2001)

5. Prince, Frank. "Translating Security for Managers." May 2001. URL: http://www.infosecuritymag.com/articles/may01/columns_secmarket.shtml (28 Oct. 2001).

6. Price, Dick. "A new standard in information security management Part 2: An examination of detailed controls." 15 May 1999. URL: http://www.itaudit.org/forum/standards/f210st.htm (3 Nov. 2001).

7. Zabarov, Dev. "Computer Security Isn't Just Computers, Part 2." 7 June 2001. URL: http://www.itworld.com/nl/unix_sec/06072001/pf_index.html (28 Oct. 2001).

8. Shaw, Erich, Jerrold Post, and Kevin Ruby. "Managing the Threat From Within." July 2000. URL: http://www.infosecuritymag.com/articles/july00/features2.shtml (28 Oct. 2001).

9. Recent SANS' Practicals on Security Awareness:

   Kaur, Harbinder. "Introduction and Education of Information Security Policies to Employees in My Organization." 29 August 2001. URL: http://www.sans.org/infosecFAQ/aware/infosec_policies.htm

   Voss, Brian. "The Ultimate Defense of Depth: Security Awareness in Your Company." 11 August 2001. URL: http://www.sans.org/infosecFAQ/aware/ultimate.htm

Johnston, Michelle. "Security Awareness Training and Privacy." 28 July 2001. URL: http://www.sans.org/infosecFAQ/aware/training.htm

Uhr, Howard. "Leveraging a Securing Awareness Program from a Security Policy." 11 July 2001. URL: http://www.sans.org/infosecFAQ/policy/leveraging.htm

Ludwig, Katherine. "Security Awareness: Preventing a Lack In Security Consciousness." 25 May 2001. URL: http://www.sans.org/infosecFAQ/aware/lack.htm

Held, Robert. 'Security Awareness – Are Your Users "clued in" or "clueless"?' 23 May 2001. URL: http://www.sans.org/infosecFAQ/policy/sec_aware.htm

Memory, Bev. "Security Awareness – Everyone's Business." 18 April 2001. URL: http://www.sans.org/infosecFAQ/start/everyone.htm

Pretorius, Andre. "Information Security Awareness Policy." 10 April 2001. URL: http://www.sans.org/infosecFAQ/policy/infosec_awareness.htm

Nichol, Kelly. "Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users." 18 December 2000. URL: http://www.sans.org/infosecFAQ/start/awareness.htm

Hisey, Patty. "Computer Security Awareness Training…Do You Need It." 20 December 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/training.htm