Global Information Assurance Certification Paper

Security Awareness – Implementing an Effective Strategy

Chelsa Russell
GSEC Practical Version 1.4b – Option 1
October 25, 2002

Abstract

People are often referred to as the weakest link in an information security program. Through either intentional or accidental misuse of access, people often leave networks and organizations exposed. "All it takes is just one weak link in the chain for an attacker to gain a foothold into your network" (Nichol, p.1). All too often, security programs tend to focus on technical controls rather than the human element. "Your organization can be bristling with firewalls and IDS, but if a naïve user ushers an attacker in through the back door you have wasted your money" (Power, p.18).

Although the weakness that people present can never be totally eliminated, a well-planned security awareness program can help to reduce the risk to an acceptable level. It is critical that people understand their role in protecting information and information assets. This paper examines the importance of security awareness and how it supports the fundamental goals of an information security program. In addition, this paper provides a recommendation for implementing an effective security awareness strategy. This paper also spends considerable time discussing common obstacles to implementing an effective strategy. These obstacles have been derived from a combination of real world experience and research.

The Foundation - Information Security Basics

In order to understand the value and requirements of a security awareness program it is helpful to first examine a few fundamental information security principles. Security awareness is a single component of a larger security program and should map directly to its goals.

The overall objective of an information security program is to protect the confidentiality, availability and integrity (C.I.A) of an organization's information and information assets. The key concept here to consider is that *aspects* of information and information assets must be protected, not just the information or assets themselves. The CISSP Prep Guide defines these fundamental principles as follows:

- **Confidentiality** attempts to prevent the intentional or unintentional unauthorized disclosure of information.
- **Integrity** ensures that modifications are not made by unauthorized personnel or processes; unauthorized modifications are not made to data

by authorized personnel or processes; and data is internally and externally consistent.

- **Availability** ensures the reliable and timely access to data or computing resources by the appropriate personnel.

All attacks, no matter what type, are designed to compromise one or all three of these fundamental principals. For example, if a user's laptop is stolen, then an unauthorized person can read or share the information stored on the machine, affecting the confidentiality of the organization's information. They can affect the integrity by changing information and disseminating it as if it has not been changed. Finally, if the information on the laptop has not been backed-up, they can affect the availability by making the information no longer accessible to the user or organization.

Another major component of Information Security to consider is Risk Management. "It is very important to understand that the risk to an organization can never be totally eliminated. In fact, eliminating risk would entail ceasing operations", (Krutz, pg.15). Since it is impossible to eliminate risk, the main objective of Risk Management is to mitigate the risk, which means to reduce the risk to a level that is acceptable to an organization. In the case of security awareness, an appropriate level of education should be defined and implemented to reduce, not eliminate the risk that users represent. It is critical to evaluate specific education needs, in order to allocate resources in the most effective manner. A risk analysis should be performed to establish a cost/benefit justification for security protections (Krutz, pg.15-16).

The Importance of the Human Element

While confidentiality, integrity and availability represent *what* aspects of information and information assets are being protected; people, process and technology describe *how* this protection occurs. All three factors of people, process and technology play an equally important role in information security. However, technical controls, such as firewalls, often receive all of the attention and people and process are overlooked.

While firewalls and other security controls provide a very necessary baseline of protection, they can be rendered useless if a user either deliberately or unintentionally misuses their access or fails to protect resources within their control. Consider the scenario that a user is tricked into giving out their ID and password to an unauthorized person over the phone. It does not sound like a huge security breach. It is just one tiny mistake, right? Unfortunately, that is not the case. This mistake creates a vulnerability in the security architecture that could result in a substantial loss if exploited. It only takes one open door to create an opportunity for an attacker. Although a shared password was the only violation used in this example, it is important to understand that there are many ways that users can become a security weakness. In addition, when the number of authorized users is considered, then the overall potential exposure is

astounding. This is why people are a major factor in the success or failure of an information security program.

Security Awareness Goals and Objectives

The primary objective of a security awareness program is to educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets. Information security is everyone's responsibility, not just the IT security department. It is critical that users understand not only on how to protect the organization's information, but why it is important to protect that information. "People are often the weakest link in a security chain, because they are not trained or generally aware of what security is all about. Employees must understand how their actions can greatly impact the overall security position of an organization" (Krutz, pg.25). An awareness program should reinforce security policy and other information security practices that are supported by the organization. Security awareness "helps minimize the cost of security incidents, helps accelerate the development of new application systems, and helps assure the consistent implementation of controls across an organization's information systems" (Wood, pg.1).

Security awareness programs are typically broken down into two different, yet related components of awareness and training. The goal of awareness is to raise the collective awareness of the importance of security and security controls. Awareness messages should be simple, clear and presented in a format that is easily understood by the audience. The goal of training is to facilitate a more in-depth level of user understanding. Some tactics include, but are not limited to formal classroom training, one-on-one training and educational packets (Krutz, pg.25-26).

Obstacles to Success

Unfortunately implementing a *successful* security awareness program can be a difficult and seemingly impossible task. Even some of the best-architected programs are often faced with a barrage of barriers and obstacles. Before implementing a security awareness program it is helpful to understand some of these common obstacles. Methods for overcoming these obstacles will be addressed in the subsequent sections of this paper on building an effective security awareness program.

- **Teaching an old dog, new tricks** – In many organizations, security is implemented as an afterthought. Because security is not always integrated from the very beginning, users have months, weeks and even years to develop bad habits. This makes the challenge of implementing a security awareness program twice as hard. Not only do you have to educate users on security, but also you have to help them unlearn any bad habits that they may have acquired. In addition, users in this

situation tend to have extra trouble buying into the value of security. As far as they are concerned, the organization has operated just fine for many years without security. New security requirements are viewed as unnecessary changes that make their lives more difficult.

- **Security is an information technology problem, not mine** - Many users share the perception that security is the sole responsibility of the IT security department and not theirs. They tend to limit their role to the bare minimum of compliance to keep their jobs rather than rather than the big picture of what they can do to help. While adhering to policy is a good start, there is much more that can be done. It is important that users understand that the IT staff cannot do it alone.
- **Implementation of new technology** – When new technology is implemented it often requires a behavior change or new level of understanding from the user community. This alone is not an issue, however, sometimes technology moves faster than or independently from the awareness program. Often times, the awareness team is out of the loop or not adequately informed of these types of educational opportunities until it is too late. This is why it is important for the security awareness program to stress internal communications as well as ensure an emergency or crisis communication strategy is in place.
- **One-size-fits-all** – Some security awareness programs fail to adequately segment their audience and deliver appropriate messages. This is a very poor strategy that results in messages getting ignored. Users receive hundreds of messages every day from all different directions. It is critical to segment your audience and ensure that people only get the messages they need. A one-size-fits-all strategy may be easy on you, but it will not be effective.
- **Too much information** – Another common mistake is to over educate. People tend to have a threshold of how much information they can stand from any one source. If you inundate a person with a constant barrage of messages, you will most likely have the effect of turning away their attention (Krutz, pg.26). Even if you have taken the necessary steps to segment your audience, and only send appropriate messages, too much information is simply too much. You don't have to build your awareness program over night. Take the time to listen to your audiences and find the right balance.
- **Lack of organization** – Many awareness programs fail to develop consistent processes and strategies for delivering messages to users. Without a consistent style, theme and delivery it is hard for the user to engage in the program or even know what to expect. Developing consistency in your communications will help establish an identity for the program and relationship with your audience.
- **Failure to follow-up** – It is all too common for security awareness

programs to launch with a bunch of enthusiasm only to fizzle out with little success. Many programs fail to establish and maintain a regular cycle of communications. It is important to establish regular communications so that users receive regular reminders of your key messages. In addition, many programs fail to follow-up with their audiences and solicit feedback. It is critical to listen to your audience and adjust your program based on their needs.

- **Getting the message where it counts** – Often times it is a real challenge to get the right message to the right audience. This is especially true in large organizations. Even if the organization has already developed a thorough communication strategy with well-maintained process for targeted communications, this can be very difficult. Email groups based on management level and department can be helpful, but do not fully solve the problem. In some cases, although an audience has been identified, it is hard to figure out specifically *who* belongs in the audience. For example, you may have a message that you need to deliver to all programmers. Your organization may have a specific programming department, but also individual programmers in various pockets all over the organization. How are you going to identify and maintain a list that ensures all pertinent messages get to all of the programmers every time? This is difficult to say the least.
- **Lack of management support** – Obtaining management support is one of the most essential aspects of a security awareness program. Unfortunately it is also one of the most challenging (Held). In order for security messages to be effective, they *must* be supported from the top down. Even though many managers express their desire to support security initiatives, putting it into action is another story. This is due to the fact that managers have their own jobs and responsibilities. Their primary goal is to meet their business objectives and it is often hard to find room for security, no matter how much they believe security is important.
- **Lack of resources** - This usually stems from the lack of management support. Without management support, it is hard to secure adequate resources, and without adequate resources, a security awareness program is limited in what it is able to achieve.
- **No explanation of *why*** – Many security awareness programs fail to educate their users on why security is important. They cover every other aspect, but leave out the information that is most likely to motivate users to change their behavior. Users that understand why certain behaviors are insecure are most likely to take ownership of the issue and change their behavior. For example, if you communicate a new password policy that has more stringent complexity rules, users will most likely view the new policy as a pain. On the other-hand, if you also communicate to users how passwords are cracked and misused and the potential impact

that this could have, then they are much more likely to take ownership and willingly adopt the new policy.

- **Social engineering –** Last but not least. Social engineering does not necessarily impact the implementation of an awareness program, but can impact its success. It is important to address, because it specifically targets the "people link" that you are trying to strengthen.

  Social Engineering is the art of preying on natural human tendencies to trust and help others in order to obtain information that would otherwise be hard to obtain. It is human tendency to think no one would purposefully try to trick or manipulate us, but in reality social engineering is one of the most widely used forms of attack. Attackers often choose this method of attack, because it is surprisingly easy and does not take a great deal of time. Why would an attacker want to spend hours trying to crack your password when he can call you, impersonate the help desk, and trick you into giving it to him instead? Some of the most common social engineering methods include impersonation, flattery, sense of urgency and third-party authorization. It is critical to develop and implement an educational strategy that specifically addresses social engineering. Unfortunately social engineering is a form of attack that can trick even the most security savvy users (Granger, Stevens, Berg).

Building an Effective Security Awareness Program

This section outlines a recommendation of key steps for building an effective security awareness program.

Establish Security Policy

"A sound security policy is the foundation of any successful security program" (Held). Before developing a security awareness program it is critical to first document all of the high-level goals, objectives and requirements of the security program in a security policy. The policy should be written in a clear and concise manner, and accurately reflect the organization's overall posture towards security. Once the policy is created it is important that users are made aware of the policy's existence and contents. Users will also need to be made aware of an consequences on non-compliance concerning the policy (Held).

Identify Current Training Needs

The next step in developing a Security Awareness program is to identify the current training needs of your organization. This is an important step that is often overlooked or rushed. All too often, programs are built based on assumptions, rather than by *listening* to what users need. By taking the time to measure the current level of security knowledge across your organization, you will be able to determine and prioritize specific needs for training (Tipton 201-202). The following list has been slightly modified from the Information Security

Management Handbook, Security Awareness Program. It includes a list of factors that will be beneficial to identify during this step.

- User learning styles and preferences for receiving information.
- Topics of specific interest or concern.
- The current level of receptiveness or resistance to the security awareness program.
- Previous education attempts that were successful or unsuccessful (if any).
- Pre-existing vehicles of training and communication that you may be able to leverage. (There is no need to re-invent the wheel.)
- Possible allies that can help gain acceptance for the program.

By doing your homework, you will be able to design a security awareness program that makes the best use of available resources and has a high potential for success. Here are just a few methods you may be able to use in order to identify current training needs:

- Interview employees of different levels, job functions and tenure.
- Send out a survey or quiz to general users on fundamental security topics.
- Research the current level of security exposures or violations at your organization. For example, the number of laptops stolen last year.
- Perform system, application and network level audits.
- Hold face-to-face meetings with different departments.
- Walk around your facility and assess the current level of physical security. Look for unlocked offices, desks and cabinets, as well as, unsecured workstations, information, and media.

Obtain Support

Once you have established the need for a security awareness program, the next step is to obtain support from senior level management, officers and others in positions of influence and power. Unfortunately, a security awareness program can be very tough to sell. Not only is security often viewed as an obstacle to business objectives, but security awareness tends to be undervalued and overlooked component of security. It often takes the back seat, while technical controls, such as firewalls and anti-virus scanners get implemented.

There are two main objectives that should be considered in securing the support of senior level management. The first objective is money. Implementing this type of program can be very expensive. Depending on the size of your organization, you will need to secure a decent size budget to get started and

maintain the program. The second, but no less important objective is to cultivate security advocates. It is critical to find supporters that do not just lend financial aid, but through their actions can lead others to value and participate in the program. Employees are much more likely to participate in training and awareness opportunities if their manager has reinforced its importance.
In order to secure the support of senior level management, you will need to help them understand that security awareness is a vital element in protecting your organization's information and information assets. Fortunately, you have already assessed your organization's specific security awareness and training needs. By providing the results of your findings as well as industry statistics and examples, you will be able to obtain the necessary support.

Determine Audiences

The next major step in developing a security awareness program is to determine your audiences. "Not everyone needs the same degree or type of information security awareness to do their jobs. An awareness program that distinguishes between groups of people, and presents only information that is relevant to that particular audience will have the best results" (Peltier, 203). Let's face it, in today's world; we are all on information overload. Between email and voicemail, internet and television, it is easy to get overwhelmed. In order to prevent your messages from being ignored or watered-down, it is critical to segment your audience and ensure people only receive the information they need. A "one-size-fits-all" awareness program simply will not work.

User communities can be segmented in a number of ways. The following list has been slightly modified from the Information Security Management Handbook, Security Awareness Program. Some of the most common methods of user community education include:

- Level of Awareness
- Level of Technical Skill
- Job Level/Category
- Specific Job Function
- Technology, System or Application Used

The method that you choose to segment your user community is not important as long as it works for your organization. One approach that works well in large organizations is to combine a few of the methods above in order to derive four main audiences. These audiences can be broken down further as required by specific communications, but should be sufficient in defining key messages. These audiences are defined as follows:

- **Senior Management:** Top-level management

- **Management:** Middle-management and others in a leadership role
- **Technical Custodians:** Anyone who has extraordinary access, knowledge and skills pertaining to the organization's network, systems and/or procedures. They perform job functions such as system/network/user administration, hardware configuration, application development/implementation and technical support.
- **End Users:** Anyone who is authorized to use the organization's information and information systems. End Users subsume the three categories above.

Define Key Messages

Before defining individual key messages for each audience, it is important to first establish a single core message or mission statement. This core message may already be written as part of the security policy, but should be considered during this step. All other key messages should support and map back to this mission statement. Here is an example:

- It is the mission of the information security program to protect the confidentiality, integrity, and availability of the corporation's information and information assets.

The next step is to establish high-level key messages for each audience. In order to do so, you should examine your organization's security policy, and determine the core messages that pertain to the different audiences that you have already defined. These messages should not only map back to your mission statement and security policy, but also provide a foundation for additional messages. The following is an example of high-level key messages based on audience:

Senior Management

- Provide senior management level oversight and guidance around security processes.
- Promote alignment of security initiatives with business priorities.
- Ensure compliance with enterprise and business unit security policies and standards.

Management

- Develop internal processes and measures for ensuring understanding of and compliance security policy and standards.
- Examine and address potential security risks in all new and existing processes.

Technical Custodian

- Implement the policies, standards and procedures that management sets.
- Ensure compliance with security policy and standards by establishing appropriate procedures, access and requirements for end users.

End User

- Protect the confidentiality, integrity and availability of the organization's information and information assets.
- Follow the specific end user responsibilities outlined in the organization's security policy & standards.

So now that you have determined high-level messages for each audience, it is time to determine specific messages and educational needs. In doing so, it is helpful to (re) examine all of the components of your security program as well as recent security related events that may produce opportunities for education (Held). Some of the major components that you will want to evaluate include:

- Security Policy, Standards and Procedures
- Pertinent Legislation (i.e. GLB, HIPAA)
- Recent Events, such as a virus or worm.
- Results of system, application and network level audits
- Requests for training or education
- Implementation of new technology
- Other findings from step one, “Identify Current Training Needs”

A few particular security topics that you may want to consider are:

- Passwords
- Physical Security – at work facility, outside of work facility
- Social Engineering
- Viruses, Trojans and Worms
- Virus Hoaxes and Spam
- Email and Internet Usage
- Unauthorized Software and Hardware
- Access Control – principle least privilege, separation of duties, and back-

up procedures

- Business Continuity and Disaster Recovery

This particular step will be an on-going process, but should be performed as an initial step in establishing the baseline awareness program. The components listed above should always be under evaluation to determine any new educational needs. The security program should be flexible and capable of re-prioritizing content and messages as needed. Remember to create communications that are appropriate for each audience. Be sure to write to a level that each audience understands. Also, by including evidence such as real would and personal examples, you will be able to generate additional interest in your communications.

Define Available Communication Vehicles

The next step in developing a security awareness program is to define available communication vehicles. Every corporation has a unique set of available vehicles so you will want to discover what is available to you. In addition, it is important that you become aware of any procedures, guidelines or requirements linked to any of these vehicles. For example, some organizations require legal approval for any company-wide emails or publications. Understanding the "rules" in advance will help you plan your efforts accordingly. Some common communication vehicles include:

- Broadcast e-mail
- Targeted e-mail
- Broadcast voicemail
- Company newsletter
- Departmental newsletter
- Intranet
- Printed materials - posters, bulletin boards and brochures
- Face-to-face - meetings, presentations, training and Security Conference/Fair
- Library - videos, books and interactive presentations
- Reminders - login-banner, marketing paraphernalia (mugs, pens, mousepads, keychains, sticky-notes, etc.)

In choosing your communication vehicle, it is important to consider your audience and remember that different people learn in different ways. It is a good idea to use multiple vehicles for any one message so that it can reach the broadest number of individuals within the given audience (Held). It is also a

good idea to fully research your available vehicles and determine any limitations or scenarios in which they cannot be used or would not be effective. For example, if your organization has remote workers that are unable to attend face-to-face presentations, then you will need to find another method to provide the information to them.

Develop a Strategy for Implementation

The final step in implementing a successful Security Awareness program is to develop a framework for consistent and effective delivery of your messages. Without this step, communications may come across as disorganized and haphazard. In order to develop an appropriate strategy, you should consider your audiences, key messages, and available communication vehicles, and determine ways to package the program into repeatable processes.

As part of this step, you should define a clear marketing strategy. The marketing components might include: a logo, slogan, common look-and-feel and templates. This will not only enable you do deliver consistent and clear messages, but will also enable your audiences to develop an understanding of what to expect. In addition, your audiences will be able to provide more valuable feedback on the information that they receive.

Remember, a Security Awareness Program consists of two major objectives: to increase awareness and facilitate understanding through training. The overall framework should be built with this in mind.

Awareness Strategy

The goal of awareness is simply to make users aware of the need to protect the information and information assets of the organization. The following is a list of repeatable tactics that can be part of your awareness strategy.

- New Hire Packet
- Monthly Newsletter
- Quarterly Lunch & Learn Presentations
- Annual Security Conference/Fair
- Incentive Program - to recognize security related achievements
- Games, Puzzles and Contests

Training Strategy

The goal of training and education is to facilitate a more in-depth level of user understanding. The following is a list of repeatable tactics that can be part of your training and education strategy.

- Basic End User Training Course
- Technical Training Courses
- Advanced Information Security Training - This training is for security practitioners and information systems auditors.
- Quarterly Education Package – This vehicle should focus on one topic each quarter that has been identified as a specific area of weakness. It should have the ability deliver specific messages for each audience concerning the chosen topic. It should also strive to provide a more thorough level of information than awareness materials.

Ability to Measure

Measurement is the final aspect of a security awareness program that needs to be addressed. It is critical that a baseline of current user understanding is established at the beginning of the program in step one, so that you will be able to determine successes and failures (Tipton, pg.201). Baselines should also be performed before implementation of any new strategies or content. Measuring education and awareness is not always straightforward so you will need to be creative. You will be able to derive some quantitative results, but will also have to rely on qualitative.

Conclusion

The state of information security is only growing more complex with time. New viruses and vulnerabilities are reported every day. McAfee Security reports, for example that on average 500 new viruses are discovered each month. With the acceleration of technology and attacks, it is becoming even more apparent that users lack the appropriate level of awareness and training opportunities. Many users have little to no understanding of their responsibility to protect information and information assets. It is critical that organizations understand the value of a security awareness program and make a commitment to closing the education gap. A well-designed and maintained security awareness program can have a great impact on strengthening the weakest link.

References

Wood, Charles Cresson, CISSP, CISA. Information Security Policies Made Easy, Version 7. San Deigo: PentaSafe Security Technologies, Inc., 1999.

Krutz, Ronald L., Russell Dean Vines. The CISSP Prep Guide. New York: John Wiley & Sons, Inc., 2001. 1 – 26.

Peltier, Tom. "Security Awareness Program." Information Security Management Handbook, 4th Edition. New York: Auerbach, 2000. 197 – 212.

Allison, Kelly. “Implementing User Security Awareness Training.” 4 Mar. 2002.
URL: http://www.giac.org/practical/kelly_allison_gsec.htm (11 Oct. 2002)

Held, Robert. “Security Awareness – Are Your Users “clued in” or “clueless”?” 23 May 2001.
URL: http://rr.sans.org/policy/sec_aware.php (11 Oct. 2002).

Nichol, Kelly. “Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users.” 18 Dec. 2000.
URL: http://rr.sans.org/start/awareness.php (14 Oct. 2002)

Daniels, Jack. “The Weakest Link….This is Not A Game!” 9 Aug. 2001.
URL: http://rr.sans.org/securitybasics/link.php (16 Oct. 2002)

“Virus Detection and Prevention Tips.” McAfee Security.
URL: http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/anti-virus-tips.asp (24 Oct. 2002).

Granger, Sarah. “Social Engineering Fundamentals, Part I: Hacker Tactics.” 18 December 2001.
URL: http://online.securityfocus.com/infocus/1527 (19 Oct. 2002)

Stevens, George. “Enhancing Defenses Against Social Engineering.” 26 Mar. 2001.
URL: http://rr.sans.org/social/defense_social.php (19 Oct. 2002)

Power, Richard. “2002 CSI/FBI Computer Crime and Security Survey.” Computer Security Issues & Trends. Vol. VIII, No.1 Spring 2002.
URL: http://www.gocsi.com/forms/fbi/pdf.html (11 Oct. 2002) (Note: This link is to a form that needs to be submitted in order to receive a free copy of the survey.)

“The 7 Top Management Errors that Lead to Computer Security Vulnerabilities.” 14 May 1999.
http://www.sans.org/newlook/resources/errors.htm (19 Oct. 2002)

Berg, Al. “Security. Cracking a Social Engineer. Enterprising thieves use a variety of common techniques to pilfer information.” 16 Aug.1999.
URL: http://packetstormsecurity.nl/docs/social-engineering/soc_eng2.html (20 Oct. 2002)

Helsing, Cheryl. Swanson, Marianne. Todd, Mary Anne. Computer User’s Guide to the Protection of Information Resources.
URL: http://nsi.org/Library/Compsec/usergide.txt (24 Oct. 2002)