Successfully Managing Cyber Security
James B. Johnson
September 12, 2001
GSEC v.1.2f

Purpose

Managing a cyber security program involves physically protecting your company's investment in computer hardware, ensuring system availability, verifying information integrity, and securing confidential information. Implementing a comprehensive verifiable program is challenging. A new Computer Security Manager should address priorities in order: learn the basics; implement policies and plans through effective management; and work diligently to publicize security practices throughout the organization.

Background

For the past year I have been challenged as a new Computer Security Manager (CSM). The CSM position has been challenging because I had very little computer security experience, and the organization had previously been downsized due to budget cuts. This challenge required that I draw upon my education as an electrical engineer, as well as, my hands-on and management experience. This included maintaining process controls in a wide range of manufacturing facilities, managing a program providing over 10,000 desktops company wide, and developing plans and programs for maintaining and supporting all process control and infrastructure computer systems for a $3 billion manufacturing facility. The focus on ensuring continuous production in these areas carried over into management of cyber security: all systems must be continuously and fully protected without impeding production goals.

In creating a cyber security management program, the size, complexity of the organization, and the sensitivity of the company's information must be taken into account. The CSM must face constant challenges to address emerging priorities; daily fire fighting can distract from the goal of implementing effective security, company wide. With that in mind, the new CSM must stay focused on implementing the first steps in a comprehensive security program as outlined below while addressing constant emerging issues and maintaining the integrity of existing protections.

Policy Authorizing the Cyber Security Manager

Because the CSM's work impacts the entire organization, a policy authorizing the cyber security program must be established and circulated throughout the organization. SANS (System Administrators, Networking, and Security) Institute, a leader in managing the threat to information systems through preparedness and response, explicitly and strongly suggests throughout both the Information Security Kickstart and SANS Security Essentials courses that the system administrator should always have permission in writing before running certain applications. (1)(2) These include but are not limited to: applications that test the security of systems and networks (such as password crackers to test the strength of user passwords); vulnerability scanners to test the security stance of individual systems attached to the network; and war dialers that test for modems set for auto-answer. Similarly, the CSM should be protected and legitimized by a policy document clearly stating his authority. The structure of the company's policy documents defines the required format and appropriate title for this document. The policy authorizing the cyber security manager should be signed by at least two levels of management above the CSM position. No matter how many levels up, the person whose authority clearly and irrefutably encompasses all areas affected by the CSM's actions should always sign it. A CSM for a complete corporation needs the policy signed by the President or CEO. A CSM of a manufacturing facility needs the signature of the plant manager.

The policy document establishing the CSM's authority should be concise and to the point. It should be distinct from the associated implementation procedures. Implementation documents are more detailed and are developed in accordance with the policy document. A letter formally appointing the CSM should be circulated throughout the organization. This documents the specific person authorized as the CSM. The relative short amount of time required to write and have this document in place is well worth the investment.

Documented Cyber Security Plan

Following the policy document, CSMs must develop a Cyber Security Plan (CSP). Having this document is critical to implementing a successful cyber security organization. Even a high-level document will be useful to upper management in assessing the value of the cyber security program. The CSP also helps the CSM document what areas of the program will be addressed. As each area is addressed (i.e., policies, implementation procedures, firewall, intrusion detection, malware, minimum security configurations, vulnerability scanning, war dialing, media clearing, etc.) the plan should be expanded to include details of how each program will be improved. The plan should also include a statement that emerging issues will be reviewed and that corrective action will be added to the plan as deficiencies are noted.

Partnering with Information Technology Management

Some organizational structures have Cyber Security in the Information Technology Division and some have it in a separate Security Division. In assuming the CSM role, take steps early to establish rapport with other managers. This especially applies when Cyber Security is in a separate division from those managers responsible for developing, maintaining, and supporting the computer systems and information that the CSM must ultimately protect. Change will be needed to implement the practices necessary to have a strong cyber security program. Having a broad range of management support in establishing, implementing, and enforcing cyber security policies and procedures will break down barriers and make managing the cyber security program much easier.

Policy Governing Cyber Security Practices

The Cyber Security Manager should put in place a set of well-written cyber security policies that determine the basis for the programs to be implemented. The policies should also explain what is expected from managers, employees, and the Cyber Security organization. (3) These policies should be written at a high level for flexibility (not to lock in specific products or force frequent procedure updates.) The policies should be carefully worded and specific enough to ensure that management's expectations for cyber security are stated explicitly. Write the policy in plain English avoiding legalese and keep the wording as simple as possible. (4) This will help everyone understand the reasons for requiring implementation. Avoid mixing policy and implementation procedures. For example a good policy might state, "All personal computers are required to run antivirus software that is updated at least monthly or more frequently as directed by the CSM." An implementation procedure would then provide specifics such as the antivirus software approved for installation, who is responsible for initial installation and subsequent updates, and what actions should be taken if malware is discovered. An example format can be found at http://www.sans.org/y2k/sec_policy.htm (5).

Implementation Procedures

Implementation procedures follow from the policy statements. When I took on my current position, there were outdated policy statements and implementation procedures for the corporation. Implementation procedures for the internal operations of cyber security were practically non-existent. After evaluating the overall performance of the new organization and the corporation as a whole, updating the corporate policy and implementation procedures became critical for three reasons. 1) Procedures are derived to implement policy: without a strong policy, any existing procedure has no backbone. 2) Under outdated policy and implementation procedures, people throughout the corporation were confused on what was expected of them and were becoming frustrated with cyber security as a whole. Now that's dangerous! 3) The majority of cyber security staff had been in the organization for over five years and knew how to do their jobs making the development of internal procedures less critical. It took six months to improve the corporate policy and implementation procedures. Since the updated corporate policy is in place, business requirements are driving the increasing size of the cyber security organization. With less experienced staff arriving it is time to increase consistency and overall performance of the organization by documenting the well-established business practices with implementation procedures. As organizations are at different maturity levels in cyber security, the focus area for policies and procedures may be different. However, ensuring that policies precede and drive procedures is the same for all organizations.

Perimeter Management

Most people who are responsible for protecting something very important would lock it up in a box and keep the key around their neck both night and day. In the computer security arena, however, the key is in danger of being duplicated or the lock broken or another means to enter the box is invented. The perimeter is not so easily secured.

The firewall is the most important device used to actively protect the perimeter. Because it enforces the access control policy for the network, it must receive strong management emphasis. The following items should be considered when first reviewing the company's firewall implementation:

- Meet with the firewall expert(s) and become familiar with the type of firewall at your facility. Top rated firewalls include Raptor Firewall, Firewall-1, and PIX Firewall. (6) If there is only one firewall expert, consider investing in a second. A second knowledgeable person will help reduce configuration errors that introduce vulnerabilities into the firewall.

- Understanding the type of firewall (whether its network layer or applications layer), evaluate whether the protection and performance meets the policy statement developed for the firewall. (7) If there is no firewall policy document, this is a good time to work with others in the corporation to establish one.
- Make sure that support is provided for the firewall 24x7 and strongly consider functionality that allows the firewall to page on-call firewall support. One cannot be over prepared. Be prepared to handle the attack that occurs when you least expect it. It isn't if an attack will happen it is when an attack will happen and how you will respond!
- Consider attending a general training course on firewalls and a course specific to your firewall. This will allow a greater understanding of how firewalls work and will allow the manager to become more involved in the rule base that governs firewall policy. A firewall cannot be better than the rule base that governs its operation.

Intrusion Detection

Intrusion detection is essential in determining whether or not the firewall has been compromised. Intrusion detection can be placed into two categories, network-based and host-based. The size and complexity of the network and systems that are to be protected will determine the overall strategy and type of detection that should be implemented. For a large complex network with hundreds of connections, I recommend emphasizing a network-based solution and then pursuing defense-in-depth with host-based detection on systems that process critical information or information that is essential to the well-being of your organization. Deploying host-based detection can be relatively inexpensive. However, support for host-based detection can become cost-prohibitive as the number and types of solutions required increase. Consider similar steps as outlined in the firewall discussion such as 24x7 support and attending both general and product specific training courses. An excellent source for more information on intrusion detection can be found at http://www.cert.org/.

Minimum System Configurations

Ideally each and every computer system should have a plan that explicitly defines the protection measures required to ensure the physical security of the system as well as cyber security of the data. This may be feasible for organizations with few systems, but for larger organizations this may become unmanageable and cost prohibitive. A viable alternative that should be considered is minimum system configurations specific to the operating platform (i.e., Unix, Win9x, WinNT, etc.). These can be written and maintained by the cyber security organization and distributed internally to system administrators and others responsible for system configurations. Configuration documents should include, at a minimum, what version(s) of the operating systems and which service packs or patches are required to be installed. Cyber Security should update these configurations at least monthly to include the latest virus definitions and security patches. When specific vulnerabilities are found to exist in the configuration, system administrators should positively confirm that systems under their control have been updated. Though a full discussion is beyond the scope of this paper, vulnerability scanning should be used to verify that minimum system configurations are in place. Some common network-based vulnerability scanners include Internet Security Systems "Internet Scanner," Axent Technologies "NetRecon," and Worldwide Digital Solutions "SAINT." For more information on vulnerability scanners, visit http://www.sans.org/tools/tools3.htm. When coupled with vulnerability scanning, minimum system configurations can be an effective tool in implementing a standard set of system specific security requirements.

Often Overlooked Areas of Cyber Security

Though the items discussed here probably will not be the highest priority for the new CSM, their inclusion in the overall cyber security program is essential in developing and maintaining an overall comprehensive program.

Media Clearing - A strong program is needed to clear media at end-of-life when it has been used to process sensitive information. End-of-life should include when the system is not longer needed and will be excessed, or if the system is being shipped for repairs. This is particularly applicable to personal PCs. Though it would be nice if all users knew how to use shredding programs such as BC Wipe (8) and other clearing programs such as Norton's Diskwipe, the reality is that many users simply are not trained to effectively utilize these tools. Therefore, I highly recommend that systems used to process sensitive information be tracked, and a complete disk wipe is performed by the cyber security group at the end-of-life. For added protection for those systems that protect highly sensitive information, consider physically removing and degaussing hard drives or send them through a shredder.

Personal Computers for Company Business - Unless critical to overall business success, do not approve a policy that allows company information to be processed on employee-owned systems. With the rapid expansion of 'always connected' to the Internet with cable modems and DSL and the lack of personnel firewalls, most home PC's are highly vulnerable, and business information placed on them should be considered compromised. If clearing of media as discussed above is appropriate for your organization, it will be very difficult to implement the same criteria for the home PC. Few employees understand the vulnerability of the information that may still reside on the hard drive when the system or hard drive is replaced, and those that understand do not know who would be responsible for clearing the hard drive. Though it may appear to be expensive and cost prohibited, if a company has valuable information that must be protected, a strong argument can be made for supplying employees company owned systems when needed for company business.

Conclusion

Successfully managing a Cyber Security Program requires addressing shifting priorities brought about by constant shifts in threats, known vulnerabilities, and the associated risk. The new Computer Security Manager must learn to manage these shifting priorities while at the same time implementing an overall comprehensive Cyber Security Program strategy. By learning the basics, implementing policies and plans through effective management, and working diligently to publicize required security practices throughout the organization, the new CSM will be well on the way to implementing a successful program. Addressing these key issues head on will help place the new manager on the road to success.

References:

(1) Fried, Stephen. “Information Security Kickstart.” SANS GIAC Training Certification

(2) Northcut, Stephen. “SANS Security Essentials.” SANS GIAC Training Certification

(3) “Information Security Policies & Computer Security Policy Directory.” URL: http://www.information-security-policies-and-standards.com/

(4) McMillian, Rob. “Site Security Policy Development.” URL: http://secinf.net/info/policy/AusCERT.html

(5) SANS Global Incident Analysis Center. “Security Policy Research Project.” URL: http://www.sans.org/y2k/sec_policy.htm

(6) Morrissey, Peter. “Seven Firewalls Fit for Your Enterprise.” Network Computing. URL: http://www.networkcomputing.com/921/921f2.html

(7) Curtin, Matt and Ranum, Marcus. “Internet Firewalls: Frequently Asked Questions.” URL: http://www.interhack.net/pubs/fwfaq/

(8) Kinney, John. “Securely Deleting Files.” URL: http://www.sans.org/infosecFAQ/privacy/deleting.htm