Global Information Assurance Certification Paper

Implementing a Comprehensive Security Program in an Existing Environment

Scott Keim

GSEC Practical Assignment Version 1.4
September 9, 2002

Abstract

The definition of information security is "measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data, or capabilities" [1]. To enable information security in your environment you need to have a defined security process by performing the following tasks: assessment, policy, implementation, training, and audit. This security process is an ongoing process that is never ending. The problem is that most companies in today's environment never started a comprehensive security program at the creation of their IT department and now must go back and retrofit this process into an already established computer infrastructure. This paper will focus on the steps to implement a comprehensive security process in a mature, established computing environment.

Introduction

Throughout your security process you will need to achieve three major security objectives [2]:

- **Confidentially** – making sure that your company's private data stays private.
- **Integrity** – the assurance that information can only be accessed or modified by those authorized personnel.
- **Availability** – insuring that systems and data are accessible when needed.

To accomplish the above objectives you will need a solid security process in place. In most of my readings about security strategies they list 4 or 5 basic steps in defining a security process to protect your company's assets and investments. These steps are:

- **Assessment** – identifies the risks present in an IT environment and recommends changes to manage and reduce this risk.
- **Policy** – provides written rules that states how systems should be configured and how employees of an organization should conduct business using information technology.
- **Implementation** – work that makes sure that systems comply with policy.
- **Training** – training end users to understand the user requirements of the information and security policies.

- **Audit** – provides a record of past events. This will help in determining if security has been compromised.

These steps need to be included in your security process from the initial assessment phase to an ongoing phase in your environment. The above process only defines the fundamental steps that need to be examined and leave out very essential steps that should be included in developing a more complete security program, especially in already established computing infrastructure.

Below is a list of essential steps that I have determined is needed to complete a more comprehensive security program:

- **Assessment and Obtain Current Configuration**
- **Develop Standard, Secure Configuration**
- **Policies and Procedures**
- **Gap Analysis**
- **Feasibility Assessment**
- **Implementation**
- **Training**
- **Administrate**
- **Audit and Monitor**

Assessment and Obtain Current Configuration

The first step in the security process that needs to be performed is the assessment. The assessment phase will answer the following basic questions of "What do we have?", "Where are we?" and "Where are we going?" In this assessment phase you need to identify:

- All of the parts of the computing environment.
- Determine their current configuration and value.
- Determine the threats of these assets.
- Identify all vulnerabilities.
- Identify the risk of these vulnerabilities.

The items that need to be evaluated in the IT environment include:

- The entire network:
  - Routers
  - Servers
  - Workstations
  - Applications
  - Firewalls
  - Handhelds

- Physical security:
  - How secure are the servers?
  - The desktops?
  - The applications?
  - The data?
- Existing policies and procedures

Once you have identified your assets and have the configurations in hand make sure you identify the business risk. Business risk is defined as **business value** x **vulnerabilities** x **threats** [3]. Each asset in the computing environment will have a different business risk. Make sure you have a good understanding of the risks associated with each asset so that you can develop a well-rounded and complete secure configuration.

Develop Standard, Secure Configuration

Once you have obtained the current configuration of your environment you will need to develop a standard and secure configuration baseline using security best practices. You can find many security best practice guidelines and benchmark tools from the following locations on the Internet:

- **http://www.cisecurity.org/** - The Center for Internet Security. Have great benchmarking tools.
- **http://nsa1.www.conxion.com/** - The National Security Agency, Security Recommendation Guides. Have excellent guidelines for your computing environment.
- **http://www.microsoft.com/security/default.asp** - Microsoft's Security & Privacy homepage. This is an excellent page that covers Microsoft best practices, etc.
- **http://www.sans.org/SCORE/** - SANS/GIAC Security Consensus Operational Readiness Evaluation website. This is an outstanding site that lists best practices and minimum standards benchmarks for the industry.

Since you are reviewing and evaluating an already established computing environment, the current configuration and the standard, secure configuration which you are developing might be one and the same. I have found that it is seldom that the current configuration meets a newly derived security standard, but it is a possibility.

Most IT professionals currently use some type of tools or documents to establish a baseline when they build routers, servers or workstations, but most forgot that this baselining document is a "living" document that becomes out dated very quickly. So revisiting these websites above and reviewing your baseline documents need to occur on a quarterly basis, at a minimum. Once you have

completed this development phase, you need to build policies and procedures to enforce your standards.

Policies and Procedures

You need to formulate policies and procedures to enforce these secure configurations for your organization's business practice. "Policies define the "What" in our business and have to be controlled, whereas the procedures define the "How to"" [4]. These policies and procedures will be the baseline for your implementation. Without policy, there is no plan upon which an organization can design and implement an effective information security program. Policies define the behavior and procedures provide the steps of implementation. Please review any existing policies and procedures that you currently have in place and at a minimum you need to develop the following [5][6]:

- **Security Policy** – "to inform users, staff and managers of their obligatory requirements for protecting technology and information assets" [7].
- **Information Policy** – Identifies the sensitivity of information and how sensitive information should be handled, stored, transmitted, and destroyed. This is the "why" of the security program.
- **Acceptable Use Policy** – Provides the company policy with regard to the appropriate use of company computer systems and resources.
- **Anti-Virus Policy** – Defines guidelines on virus protection software on the organizations computing environment (servers, workstations, handhelds, etc.).
- **Audit Policy** – Defines the requirements and provides the security team authority to perform audits and monitor activities in the organization's environment.
- **Password Policy** – Defines guidelines for creating, administrating, and changing passwords within the organization.
- **Dial-in Policy** – Defines the appropriate dial-in use and access.
- **Router Security Policy** – Defines the standards for minimum router security configuration within the organization.
- **Server Security Policy** – Defines the standards for minimum server security configuration within organization.
- **Workstation Security Policy** – Defines the standards for minimum workstation configuration within the organization.
- **Physical Security Policy** - Defines the minimum guidelines to secure the computing environment within the organization.
- **Firewall Policy** – Defines the rules for configuring and setting up firewalls within the organization.
- **Backup Policy (and Procedures)** – Identifies the requirements for computer system backups.
- **Disaster Recovery Plan** – Provides the guidelines for recreating the computing environment after a disaster.

- **User Account Management Procedures** – Defines the steps to add/remove users from the computing systems.
- **Incident Response Procedure** – Identifies the goals and steps in handling an information security incident.
- **System Configuration Guidelines** – Identifies the basic configuration guidelines for building secure computing systems.
- **Software Development Methodology** – Defines the methodology of the organization's software development process.

Policies and procedures should cover all aspects of the organization's operations. It is highly likely that various aspects of the organization's computing environment were not considered or possibly not in existence when the original policy or procedure was created, so it is critical to create or modify these documents. Once you have established solid policies and procedures you will need to perform a gap analysis between your current configurations and the newly created secure configurations.

Gap Analysis

A gap analysis "is the study of the difference between two different information systems or applications, often for the purpose of determining how to get from one state to a new state" [8]. This step will take place after you have finished the policy and procedure creation and developed a standard and secure environment. The gap analysis will show you where you are currently versus where you need to go. It will show you the gaps or holes that exist. These gaps will need to be defined during this step to give you a better understanding of how much work is required to fill the security gaps in your environment. Once this analysis is completed you will be ready for the next step: the feasibility assessment.

Feasibility Assessment

With the gap analysis in hand you will need to perform a feasibility assessment. This feasibility assessment will uncover if your secure and standard configuration that you developed is attainable by reviewing the recommendations and taking into account the following factors:

- Time to implement
- Cost
- Resources available
- Difficulty of implementation

For example, by using security best practices to lock down 10 web servers in your environment you have determined that is necessary to install an edge router and CheckPoint Firewall in all 10 locations where each web server exist, but after

the feasibility assessment the cost might outweigh the benefit. Most likely when this occurs you will have to modify your new design where all of the facts of money, resource, and time make sense. A modified design to my example might be to move all of the web servers to 1 or 2 locations so that only a 10% of the original cost is needed for the new equipment. This redesign will also take less time to implement and will be easier to administer.

During this feasibility assessment is the time to modify your original design and recommendations, if needed. Also, you might need to modify some of the policy and procedures that you have created. They might be too strict and not attainable or enforceable.

Just keep in mind, some companies cannot afford large-scale security implementations. It all boils down to what is it risk? and how much will be lost if this data gets compromised? Since each company is different, these questions will need to be answered by you and your management. Once the feasibility assessment has been approved it is time to implement the your new secure configurations.

Implementation

During this step you will need to evaluate and prioritize by business risk which assets needs to be addressed or implemented first. After you have developed this priority list you will need to develop a strong project plan identifying the resources needed to meet the timeframe that was defined.

Some larger companies will hand over the implementation phase to their Operations Group or to a project manager that is on staff, but make sure that you, as the security officer/administrator, stay involved to make sure that the implementation happens properly.

Depending on the security state of your environment and how much work needs to be implemented, this is the time that you will need to start educating the employees and IT staff about the newly formed policies and procedures.

Training

One of the most important steps in a successful security program is training the employees to a higher level of security awareness [9]. Employees need to understand data security and why it is important to your company. After some type of IT security training, whether it is classroom or online, each employee needs to be tested or signoff that he/she understands the security policies and will abide by them. This way the employee can be held accountable if data security is compromised in the future.

Some very important statistics that need to be included in your training include the "Computer Crime and Security Survey" conducted by CSI. Some highlights of this survey reveal [10]:

- 98% of respondents detected computer security breaches within the last twelve months.
- 80% acknowledge financial losses due to computer breaches.
- 44% of the respondents were able to determine that they totaled $455,848,000 in losses.
- 74% cited that their Internet connection was a frequent point of attack (33%).
- 78% detected employee abuse of Internet access privileges.
- Etc.

Administrate

Now that the employees are aware of the new security policies, and you have implemented the new secure configuration, you need to administrate your environment.

Many IT professionals believe that once you have installed a secure environment that their work is over and their computing environment is safe from hackers, etc. Well, they are mistaken. Almost daily new vulnerabilities are being discovered in operating systems, applications, etc. You, as the security professional in your organization, need to get stay on top of these vulnerabilities and make sure that you are protected at all times. One way to stay informed and alerted is to subscribe and visit to many of the security websites that post daily and weekly newsletters of newly found vulnerabilities and holes in the computing environment. Here is a list of my top sites:

- **http://www.sans.org/newlook/digests/** - SANS Institute Security Digests Website.
- **http://www.cert.org/** - CERT Coordination Center Website.
- **http://www.sarc.com/** - Symantec Security Response Website.
- **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp** - Microsoft's TechNet Product Security Notification Website.
- **http://isc.incidents.org/** - Internet Storm Center Website.
- **www.ntbugtraq.com** – NTBugTraq Website.
- **http://www.sans.org/newlook/resources/** - SANS Institute Resources Website.
- **www.searchsecurity.com** – Search Security.com Website.
- **www.infosyssec.org/infosyssec** - The Security Portal for Information Security Professionals Website.
- **www.foundstone.com** – Foundstone Security Website.

- **www.cve.mitre.org** - Common Vulnerabilities and Exposures Websites.
- **http://www.hackers.com/** - Hackers Website. Please note that this site could be dangerous to your workstation or network. Please access from a secure, isolated pc.

Administrating your secure environment is not brain surgery but you need to be aware of newly found threats to your network and make changes to your environment to protect the data from these dangers.

Audit and Monitor

Auditing and monitoring your computing environment is an extension of the last step of administration. Auditing is needed because no matter how secure your network environment is, there is always the possibility that a breach may occur [11]. Like I mentioned in the last step, there are always new vulnerabilities and new tricks that hackers find to compromise a network environment. You need to stay abreast of the trends in the hacking world to keep your environment and data safe.

Make sure that on all of your routers, servers, and workstations, that auditing is enabled and that it is capturing all the vital information like "who logged in successfully?", "who logged in unsuccessfully?", and "what did they do or go?" These audit logs are very important in tracking down unauthorized breaches and preventing them, as well as having legal documentation for the human resources department if policies have been compromised and they need act upon them.

Even though auditing is enabled you need to monitor these logs on a daily basis for them to be effective. Just capturing the information is not good enough if you do not know what the log details entail. These audit logs need to be reviewed for any suspicious behaviors and if any action if needed. You as the security professional need to take the steps to research and stop these breaches.

Auditing and monitoring is a vital and ongoing process in the security program. Just as your computing environment dynamically changes with the addition of equipment, etc., your audit logs are dynamically changing with additions of breaches. I can not stress this point enough - make sure you know what is happening in your computing environment at all times!

Conclusion

Implementing a comprehensive security program in your computing environment is not an option, it is a necessity. Every security professional needs to revisit their current environment on a regular basis to ensure that holes have not been opened.

If you follow the steps and phases that I have listed throughout this document you will have a complete picture of your computing infrastructure, the current security measures taken to secure the data in your environment, and the processes that it takes to keep these assets secure by the ongoing steps of auditing and monitoring. Security is a crucial necessity in any computing environment, but if you do not have a complete program your network and data will become compromised from the outside or from within. Please take the essential steps to secure your network environment. Like I mentioned earlier in this paper, security is not brain surgery, but if you follow the above steps you will be much closer to securing your companies assets, which I am sure your company will appreciate.

Bibliography

1. Maiwald, Eric. Network Security: A Beginner's Guide. New York: Osborne/McGraw-Hill, 2001. 4.

2. Benson, Christopher. "Security Strategies." 2000. URL: **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpent/sec1/secstrat.asp** (7 September 2002).

3. Piepers, Eric. "Cost-effective Information Security (Information Security from a business perspective)." June 6, 2001. URL: **http://rr.sans.org/audit/cost-effective.php** (7 September 2002).

4. Farra, William. "Security Awareness Starts in IT." September 2001. URL: **http://rr.sans.org/aware/IT.php** (7 September 2002).

5. Crabb-Guel, Michele. "Building An Effective Security Infrastructure." URL: **http://www.sans.org/newlook/resources/policies/policies.htm** (9 September 2002).

6. Maiwald, Eric. Network Security: A Beginner's Guide. New York: Osborne/McGraw-Hill, 2001. 59-74.

7. Parmar, S. K. "An Introduction to Security, Security Manual." 1999. URL: **http://downloads.securityfocus.com/library/** (9 September 2002).

8. Whatis.com. URL: **http://whatis.techtarget.com/definition/0,,sid9_gci831294,00.html** (9 September 2002).

9. Geiger, Robert. "Back to Information Security Basics." 2000. URL: **http://users.bestweb.net/~bgieger/art_paper/wp_backbasic.htm** (8 September 2002).

10. Rapalus, Patrice. "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row." 2002. URL: **http://www.gocsi.com/press/20020407.html** (8 September 2002).

11. Davies, Alan. "Security from Scratch…How to Achieve It." September 2001. URL: **http://rr.sans.org/securitybasics/scratch.php** (8 September 2002).

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event