Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Creating an Information Systems Security Policy

This paper addresses the steps necessary for creating an Information Systems (IS) Security Policy.

Copyright SANS Institute
Author Retains Full Rights

AD

Walter F. Patrick
GSEC Practical Assignment
Version 1.2f

Creating an Information Systems Security Policy

Background:

Over the years I have been exposed to many different concepts as to what a Computer Security Policy "is" or more, what a Computer Security Policy "should be". The Government, the Department of Defense (DOD) to be exact, has it's own set of rules of how to write a policy (DODD). Moreover, within the government, one must follow the rules of the "higher command". It works like this; Congress passed a law, The Computer Security Act of 1987, Public Law 100-235, (CSA), The Department of Defense wrote a very broad policy stating that all the military Branches will follow the law (Public Law 100-235). Next the Departments of the Navy, Army, and Air Force, etc., wrote their own interpretation of the DOD policy. Next, the various Commands of each of the Departments of the Navy, Army, and Air Force, etc. wrote their interpretation of their respective Commands' policy and so on down the line until you get to the battalion, squad, installation, etc., level. Each lower element of the military, starting with DOD, can write a more stringent policy, but cannot undo what an upper echelon has written. Mostly, the lower echelons "interpret" the upper echelon's policy. There is very little room for anyone at the lower levels to misunderstand the policies. All this is well and good…especially for an organization as huge and as structured as the military.

But what about the private sector? How does one write a Computer Security Policy without any direction from "higher command"? It seems obvious that all one has to do is follow the Corporate Security Policy. Well… that's possible, if a Corporate Computer Security Policy exist. What if you're the one that has to write a corporate security policy?

The following paragraphs are going to be a general outline as to what should be included in an Information Systems (IS) Security Policy. This structure can be followed, whether one is writing a corporate, a departmental, or a local (branch, shop, etc.) IS Security Policy. If everyone in an a private corporation, starting at the corporate level, down to the employee level follows the same structure when writing a policy, then there should not be much room for an employee to misinterpret the policies. Be sure to get the corporate legal department to bless the new policy. It might also be wise to get the audit, contracts, and physical security departments blessings too. It would be even better if one could get those departments to help write the document.

Executive Summary:

The first paragraph in the policy should be an "Executive Summary" of the policy. In this paragraph state the objective(s) of the policy in a general overview fashion. It should state why the policy was written. What the policy covers, and equally, what the policy does not cover. It should say, by whose authority this policy been written. It should list any exceptions to the policy, i.e. if another policy covers a certain aspect, then this policy does not.

Scope and Applicability:

The next paragraph in the policy should cover the "scope" of the policy. The scope of the policy should state, who (employees, vendors, contractors, etc.) are covered by this policy, what

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

types of operating systems, communications systems, network systems, etc. are covered. This paragraph should detail who (employees, departments, etc.) must adhere to this policy. And again, what is not covered in the scope of this policy, i.e. personnel and items covered under another policy. Don't forget to include in this paragraph who is responsible to maintain this policy and to whom all updates and requests for exceptions should be directed. Also include a date, once or twice a year, when major changes to the policy may be made. An IS Security Policy is a "living" document and should have the flexibility to change often.

General Policy:

Next comes the policy itself. The first part of the policy should be a "Policy Statement" explaining, in general, why this policy is necessary. Items such as, to protect company assets from destruction or disclosure, to ensure confidentiality or integrity, are some of the items that go here. These paragraphs should state who is responsible for this policy at every management level within the company. The paragraphs should define terms used throughout the policy such as the difference, if any, between Information Systems (computers, networks, etc.) and Office Automation equipment (calculators, typewriters, etc.), if necessary. When making these determinations remember that telephones today are microcircuits controlled by computers and maybe should be included under the heading of Information Systems. (If in doubt… who owns a majority of the Internet infrastructure in this country? TeleComs!)

Roles and Responsibilities:

One of the first things that everyone needs to know is; what are their responsibilities under this policy? Under these paragraphs one should explain the roles of the different departments and individuals in following and enforcing this policy. There are basically two types of responsibilities, Organizational and Functional. Organizational responsibilities are for individuals like; Vice President in Charge of Information Systems Security, Chief Information Officer, Chief Information Security Officer, Internal Audit, etc. Functional responsibilities usually cover Project Sponsors (Managers), Chief Technology Officer, and the Information Systems Security Officer and be sure to include roles and responsibilities for all levels of management and employees.

This section could also be used to create functional roles for various individuals within an organization and to designate an IS Security Department and their roles and responsibilities.

Compliance:

One of the major items usually left out of any IS Security policy is; what happens to the department or individual that violates this policy? After having explained everyone's roles in the preceding paragraphs, now explain what happens if the policy is not followed. Such penalties as lost of the privilege to use the company's IS resources, right down to termination for flagrant disregard of policy. And make sure to explain that the penalties are the same whether the violator is a Vice President, Manager, or lower level employee. After all, someone could probably do more damage to a system or network with a Vice President or Manager's password (stuck to the side of the monitor) than with most ordinary user's password (system administrators not included).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

All the policy sections previous to this point should probably be included in the corporate policy, but not necessarily on the lower level (departmental) polices. Although, they should be cited in lower level policies.

However, <u>all</u> levels of policies should contain the following paragraphs.

Accreditation:

Although that is an impressive sounding word (the DOD likes to use it), it is nothing more than "risk assessment". It is the process where information pertaining to the security of an company's' computer systems, networks and communications systems is collected, analyzed, and submitted for approval to the highest level of management responsible for those systems.

The collected information will contain items such as:

What type of data is processed on the system (company confidential, customer or client information, etc.)?
Is the system connected to a network (a Local Area Network (LAN), or a Wide Area Network (WAN)?
Who has access to the system?
Is the system locked down when no one is around, etc?

There is plenty of documentation around for one to be able to perform a valid risk assessment (CLIR). There's even some automated risk assessment tools available over the Internet (CSCI, RiskPac) or (CSI, IPAK).

Once a risk assessment has been performed, countermeasures should be put in place to reduce the risks to an acceptable level. I.e., if a system is connected to an e-mail server or the Internet, there's a high probability that the system will receive some type of virus. Here is an article from ICSA.Net, 23 October 2000:

*"The number of corporations infected by viruses has risen by **20%** this year alone*
***99.67%** of companies surveyed experienced at least one virus encounter during the survey period*
***51%** claimed they had at least one "virus disaster" during the 12-month period before they were surveyed*
***80%** said the "LoveLetter" virus was their most recent virus disaster*
The monthly rate of infection per 1000 PCs has been nearly doubling every year since 1996
*The reported damage estimate from the "LoveLetter" virus is as much as **$10 Billion**.*
The reported damage estimate from the "Melissa" virus was $385 Million
*Including hard and soft dollar figures, the true cost of virus disasters is between **$100,000** and **$1 Million** per company."*

Does that look like a wake-up call or what? A virus may or may not destroy or compromise the data (client information, as an example) on that computer. By installing the latest virus detection and eradication software on both the e-mail server and the user's workstation, and keeping the virus definitions up to date, the risk of an infection is lowered to a level of risk that a manager should be able to accept. By the way, it does no good to install countermeasures, such as virus protection, and never test and evaluate their effectiveness. It's usually too late if the countermeasures fail.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The paragraphs on "risk assessment" should also include what are the manager's and the user's (employee's) responsibilities in performing the risk assessment, procuring and installing countermeasures and testing of those countermeasures. It may be that the manager is willing to accept the risk (foolishly, its so cheap now) of not having "virus" protection installed on the system(s).

Over the past several years, managers have come to understand the risk of "viruses", but have ignored the possibility of the systems they are responsible for being "hacked". Most managers will tell you it's not a problem there are "firewalls" between the internal network (Intranet) and the outside networks (Internet, Extra nets) or that all their Intranet's external connections are on "dedicated" private lines. Well, the FBI statistics still say that approximately 70% of the "hacking" comes from the inside (disgruntle employees…. when was the last time you hear from someone who felt they didn't get a "good enough" raise in their pay?).

> *"The FBI's national Computer Crimes Squad estimates that between 85 and 97 percent of computer intrusions are not even detected. In a recent test sponsored by the Department of Defense, the statistics were startling. Attempts were made to attack a total of 8932 systems participating in the test. 7860 of those systems were successfully penetrated. The management of only 390 of those 7860 systems detected the attacks, and only 19 of the managers reported the attacks." (Richard Power, 1995)*

Also included in these paragraphs should be the company's method of classifying the data resident on the mainframes, servers and workstations. What type of data is "Company Confidential", "Company Public", or sensitive client data? How does one classify customer information? If the company maintains a database of customer or clients does the Electronic Communications Privacy Act (ECPA, 1986) or The Computer Fraud and Abuse Act (CFAA, 1986) apply? Financial institutions and their affiliates now, since June of 2001, have to comply with the Gramm-Leach-Bliley Act (GLB, 1999) when it comes to customer information.

And the last part of the accreditation process is the contingency plan. The contingency plan usually consists of what to do if the overhead sprinkler system should go off inadvertently or if there is a natural or for that matter unnatural disaster.

There should be a risk assessment, countermeasures, applied and tested, as required, and a contingency plan for every individual piece of IS equipment the corporation owns or operates, whether it be a mainframe, a workstation, a printer, a copier, a telephone system, etc.

Risk Management:

This will probably be the largest section of the IS Security Policy as it has many elements to cover. Risk management looks at an organization's IS assets exposure to environmental risks. Risk management is continuos and must be reevaluated whenever changes occur to the IS assets' environment. These paragraphs should include such elements as those that affect the IS Security environment. Elements like the following must be included under this section:

access controls – usually descriptions of logon warning screens on a computer and access lists for dedicated computer rooms, non-disclosure agreements.
system backups – by whom, how often and where stored (offsite is best).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

incident handling – what should be reported, to whom, what will be the response, by whom.
virus protection – mandatory installation of, how often updated (automatic or manual), virus incident handling.
unauthorized access – who is allowed to access the company's computer assets and LAN
monitoring – stating who will monitor the network for internal and external intrusions, and users for violations of security policies, who has access to intrusion detection devices, who will review and/or disseminate the logs.
encryption – what is the company standard encryption methodology, when will encryption be used and by whom.
digital signatures – what is the company standard, when will digital signatures be used and by whom.
web presence – what is and is not allowed to be placed on a public web server and who is allowed to publish
disposing of resources – how to, by whom
passwords – duration, number of and what type of characters, who must use passwords, for what and when, how to create. (UNI-C)
use of personal resources within the company – allowed or not allowed, if so, under what conditions
inspections and reviews – of what resources, how often, conducted by whom
entertainment software, games, etc. – allowed or not allowed, if allowed when can be used.
removal media - CDs, floppy disk, for personal or company use and usage marked
freeware or shareware - authorized or not, if authorized, under what conditions. Excellent definitions of both shareware and freeware can be found on the Internet (CFS)
software copyrights – software copyright laws are very stringent (SIIA), who will be liable if a copyright is violated, who is responsible to ensure copyrights are not violated.
personnel/physical security – what happens if a system containing sensitive information is moved out from a locked door.
vendor responsibilities – what rules will a vendor follow when using a company IS asset or when using its own assets on company premises.
public disclosure – who can release information to the public and under what restrictions. And what about non-disclosure agreements for employees as well as vendors.
computer room facilities/areas – IS Security personnel should be involved in the design stage of new computer room facilities in order in insure safeguards to protect company IS assets.
system configuration change – changes that alter the security profile (risk) of a company IS asset should not be instituted without consulting IS Security personnel first.
audit of IS Security compliance – who will audit for compliance? (the Audit Department), how will the audit be conducted. An excellent source for auditing criteria is the Information Systems Audit and Control Association (ISACA™). They publish several auditing guidelines, some free for downloading.
security awareness and training – mandates an IS Security awareness training program, indicates who should attend this training, how often training will be conducted and what will be included in the training.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

inventory of IS assets –who should keep an inventory of all the company's IS assets, who should have access to that inventory, is it available to the risk management/audit teams
documentation – to support risk management what support documentation should be maintained, by whom and how (electronically, etc.), i.e. risk assessment, countermeasures, test results documentation, standard operating procedures(SOPs), disaster recovery/ contingency plans.

There are the beginning elements of a good security policy. I have included most of the elements that I am familiar with. I am sure there are many other elements that should be included in the policy. That's why one should include the departments mentioned previously in both the creation and enforcement of the policy.

The whole IS Security Policy should be signed by the company's Chief IS Security Officer or equivalent. And there should probably be a cover letter signed by the company Chief Executive Office/President showing support for the document. That way, there's no question whether management is behind the policy.

Bibliography

1. CSA, COMPUTER SECURITY ACT OF 1987, Public Law 100-235 (H.R. 145) January 8, 1988 URL: http://www.cio.gov/Documents/computer_security_act_Jan_1998.html

2. DODD, Department of Defense Directive 5200.28-STD, 1985.
URL: http://csrc.ncsl.nist.gov/secpubs/rainbow/std001.txt

3. The Council on Library and Information Resources, "Risk Management of Digital Information: A File Format Investigation", June 2000, Gregory W. Lawrence, William R. Kehoe, Oya Y. Rieger, William H. Walters, Anne R. Kenney.
URL: http://www.clir.org/pubs/reports/pub93/contents.html

4. CSCI, RiskPac Software, URL: http://www.csciweb.com/rip.htm

5. CSI, IPAK (requires Excel '97 or higher) URL: http://www.gocsi.com/prelea991122.htm

6. ISACA™, Information Systems Audit and Control Association,
URL: http://www.isaca.org/standard/guide19.htm

7. ICSA.Net, 23 October 2000, "2000 Computer Virus Prevalence Survey"
URL: http://www.securitystats.com/reports.asp

8. FBI, Statement for the Record of Michael A. Vatis, National Infrastructure Protection Center, Federal Bureau of Investigation, May 25, 2000
URL: http://www.fbi.gov/congress/congress00/vatis052500.htm

9. Richard Power, -Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare, Computer Security Institute, 1995.
URL: http://www.happyhacker.org/crime/crimelaw.shtml

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

10. ECPA, Electronic Communications Privacy Act of 1986
URL: http://www.digitalcentury.com/encyclo/update/ecpa.html

11. CFAA, The Computer Fraud and Abuse Act of 1986
URL: http://www.digitalcentury.com/encyclo/update/comfraud.html

12. GLB, Gramm-Leach-Bliley Act (AKA, Financial Services Modernization Act of 1999)
URL: http://www.senate.gov/~banking/conf/

13. SIIA, Software & Information Industry Association,
URL: http://www.spa.org.

14. CFS, Completely Free Software
URL: http://www.completelyfreesoftware.com/definitions.html

15. UNI-C, How to create good passwords URL: http://www.uni-c.dtu.dk/good_passwords.html

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**