Global Information Assurance Certification Paper

David Jarmon
SANS Security Essentials GSEC Practical Assignment Version 1.3
A Preparation Guide to Information Security Policies

Introduction

As a security consultant, I have witnessed many attempts to implement a successful security program. Some attempts fail because there is a lack of management support, some attempts fail because there is no enforcement, and others fail because of a lack of experience. But the most common problem is neglecting the security program once it is implemented. To name a few common problems, policies are not updated; configuration changes are not tracked; no internal audits; and a lack of a 'schedule' for implementing patches and fixes. It is very important that a life cycle approach is used, updated, and adhered to for security.

acceptable risk) of all electronic media within a company or organization. There are a few key elements that should be considered when developing security policies. Why and what data needs protection? What is the negative financial impact based upon the SLE (single loss expectancy) if a breach occurs or if the asset is lost or destroyed? This would also include a final analysis of the ARO (annual rate of occurrence). Based upon this analysis, is this policy essential and financially justified? Once the policy is justified, is it clear who is responsible for what? If implemented, will it be enforceable? Consequently, for any policy to be successful over a period of time there must designated people trained and held accountable as well as possessing the authority to carry out the policy. It is very important that all key areas are reviewed when developing any information security policy. I would like to elaborate briefly on three key areas.

Can this policy be implemented?

Is the manpower/experience available to implement and support the security proposal? Does the corporate legal department support the proposed actions? For example, if an intrusion detection system has been added to the policy, are the staff members knowledgeable about Intrusion Detection Systems (IDS)? Is the staff capable of implementing the new system? If the answer is no, then the work could be contracted out. Who is screening the IDS logs and maintaining the system? Will this require additional manpower? If management is reluctant about security, and we are suggesting a new full-time hire to administer the IDS, then it may not have the support of management. An alternate approach may be to train existing staff on the technical issues.

Another issue pertains to legal. An organization may be in a situation where they need to comply with certain local, state, and/or federal laws. Ultimately, any part of the policy that does not satisfy laws will result in a policy being disregarded. Furthermore, appropriate wording is also extremely important. For example, review the following case:

> *In a recent court case, an employee won a $175,000 settlement because she accidentally viewed what she considered to be a pornographic Web site while on the job. How did she get away with holding her employer accountable? Was the questionable site located on a company owned Web server?*
>
> *The company had a corporate policy stating that "pornographic sites will be blocked, and they cannot be accessed from the corporate network." The company was filtering out access to sites that contained what it considered to be questionable subject matter. Unfortunately, there are so many "questionable" sites on the Internet that they could*

not block them all.

> *The court ruled that the company was liable for breach of contract because it did not block all so-called questionable sites. By instituting a policy stating that it would filter out these sites, the company was "accepting responsibility for the successful execution of this activity" – and was therefore accountable. The damage award, as well as reimbursement for the employee's "distress," was based on this finding.* (Security Complete, p. 33)

These were just two of many questions that should be thoroughly answered to avoid a major "loop hole" in the policy. It is advisable to consult with the corporate legal counsel for "cause and effect" review before implementing a security policy. By doing this, the risk for litigation is greatly reduced.

Is it clear who is responsible for what?

All employees must have their respective roles outlined in the policy. All these questions must be answered in the security policy. Who is going to implement the policy? Who is going to enforce the policy? Who is going to maintain security hardware and software? Who is going to perform security checks and audits? What is the System Administrator responsible for? What are the Network Administrator's and the Security Manager's responsibilities? What are the end users responsibilities?

If implemented, will this be enforceable?

Will management and the legal department support the effort? Without management support, it is a waste of time to implement a security policy. If management is reluctant now, they will likely be more supportive once security has been breached. (*It has been stated that it's not a matter of if your company assets will be victim to a security incident, but when*.) It is an unfortunate mindset, but does frequently occur. Also, most users have no concept of security. When a policy dictates that they cannot stream their favorite radio station from across the United States, because it "hogs" bandwidth, they just laugh and do it anyway. Employees will defy security and policies, but if there are disciplinary implications enforced by management, then it has a better chance of compliance. However, management cannot always be there to enforce policy if they do not know about it. That is why it is important to monitor and verify compliance. If the Internal Revenue Service did not perform audits, how many of us would cheat on our taxes? The same is true here. Non-compliance of just one policy tends to

lead to abuse of others. To review, management and policy compliance monitoring are two very big assets when implementing security policies.

Why do I need a Security Policy?

A security policy is needed to inform users and staff members of the need and their responsibility to protect the organizations technology and critical information. Here is an excerpt from Security Complete that explains a little further:

> *A security policy serves many functions. It is a central document that describes in detail acceptable network activity and penalties for misuse. A security policy also provides a forum for identifying and clarifying security goals and objectives to the organization as a whole. A good security policy shows each employee how he or she is responsible for helping to maintain a secure environment.* (Security Complete, p. 29)

Security policies are beneficial since it is the foundation of a security program. Without policies, an organization's security program will be short lived. Security policies inform employees of the guidelines that protect company information and assets. A well-written policy will provide acceptable use and prohibited use guidelines, which will automatically reduce risks if employees adhere to the policy. Security policies also serve as a good foundation for conducting audits of the network and its resources. It serves as a baseline to follow when trying to uncover vulnerabilities or when conducting forensics activities if security has been breached. Developing a security policy will help define strategic goals, identify critical assets, and uncover potential vulnerabilities and/or existing vulnerabilities.

Management Support

A sound security policy starts with the executives at the top. Without management supporting security policies, they might as well be non-existent. In most instances, management is ultimately responsible for setting the "tone" for a sound security infrastructure.

Security policies, and security in general, are typically at the bottom of the "things to do" list of executives. They have probably heard the war stories from other executives - policies are too hard to develop, they are labor intensive and expensive, they are hard to implement, users complain and label them a nuisance, there is concern about privacy infringement, etc. In most cases it takes a serious security incident, or an exceptional sales pitch by the security manger, to gain the support of management.

It is important to be persistent regarding security policies. Do not give up! Adopt the philosophy to do "what ever it takes". In the end, the hard work and diligence will pay

off and management will surely be supportive.

What's already there: Review current policies

Remember the old saying, "Do not reinvent the wheel". This also applies to policy development. Gather up all current policies and review them thoroughly. In some cases, existing policies can be used with only minor changes. In less fortunate situations, you may have to start from scratch.

Identify and locate Company assets

Here are some questions to ask: What does the company have that others want? What processes, data, or information systems is critical to the company? What would bring the organization to a halt? The answers provided to these questions will likely represent the companies' assets. For example, assets could range from databases with critical data, application systems with vital company, customer, and/or employee information, classified information, shared drives, email servers, and web servers. Everything that is essential to running the company, or could jeopardize the company, is an asset and must be protected.

Identify threats

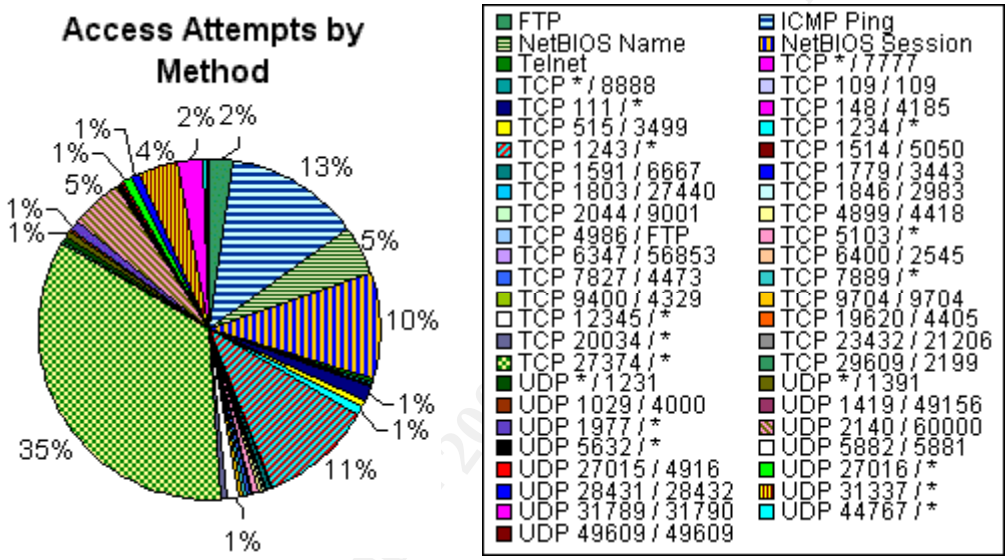
What types of threats is the company susceptible to? This may vary depending on the type of company in question, but there are three threat "characteristics" that should always be kept in mind: Confidentiality, Integrity, and Availability. Confidentiality refers to confidential information that is for certain eyes-only (i.e., managers, supervisors, select employees). It is information that should remain private to the company, and to certain employees within the company. Integrity refers to company information and/or data. It is important that it be absolutely accurate and up to date. Finally there is availability. Availability refers to the accessibility of company information and resources. It is vital that a company's information and resources be readily available.

Below is a partial list of the most common threats that can jeopardize the confidentiality, integrity, and availability of a company's assets.

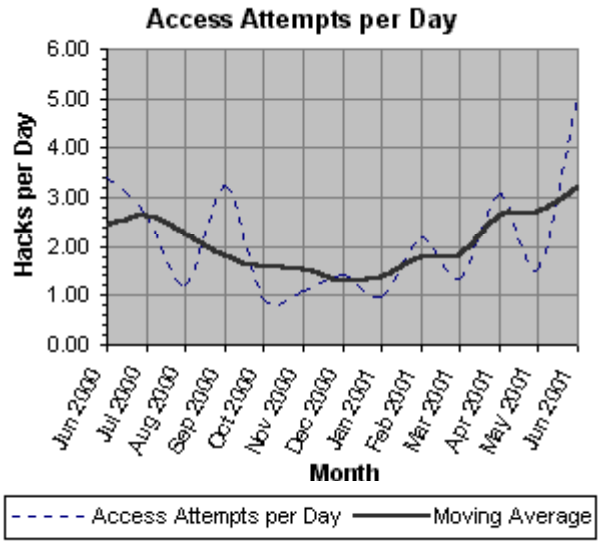
Hackers

Hackers are among the most well known outside threats to information systems. The media my portray hackers as geniuses, but in reality, they are nothing more than persistent individuals who have sufficient time to learn their craft. Hackers can be characterized into three categories: Hackers, Crackers, and Phreakers. The term Hacker can be defined as an individual that breaks into computer systems to

learn more about them. They generally do not intend harm or expect financial gain; however, they may unintentionally pass on valuable information to others, which could damage systems. The term Cracker refers to the "criminal hacker". These individuals intend to do harm to information systems. While their motives may vary, they are all out for their own personal fortune. The term Phreaker refers to an individual who prides himself or herself on compromising telephone systems. They have been known to reroute phone lines, disconnect phone lines, sell wiretaps, etc. (Winkler)



source: http://www.btinternet.com/~shawweb/george/hacks/graphs.html



source: http://www.btinternet.com/~shawweb/george/hacks/graphs1.html

Viruses/Trojans/Worms

Viruses, trojans, and worms are probably the most disruptive of the security incidents. Viruses are modifications made to existing program files that duplicate on their own**.** One example is the Melissa virus (March 1999) with an estimated damage of millions of dollars. Trojans are programs that infect systems by taking advantage of unsuspicious end users that believe they are playing a familiar game or reading email attachments. Two such Trojans were Netbus and Subseven. Worms differentiate themselves by having the ability to replicate. They typically take advantage of local area networks and email clients. A good example of a notorious worm is the morris worm created by Robert Morris in1988. While it has been estimated that some 200 viruses, trojans, and worms (or variations of) are released each week, the best defense is still properly implemented anti-virus software and a sound policy to enforce it. While there are countless vendors that offer anti-virus software, take the time to thoroughly research which piece of software will compliment the company's needs. (University of Vanderbilt)

Denial of Service (DOS)

A denial of service attack is usually an attempt to deny a user, or group of users, the ability to use a particular service. Denial of service attempts may be intentional by flooding a network to prevent traffic or unintentionally by using a company server to store large amounts of software, thus denying access to that server. A variation of this tactic is the distributed denial of service. This particular method uses several servers to attack other machines. It can be difficult to identify this type of attack because the traffic may look like valid access attempts. Both denial of service and distributed denial of service attacks can disrupt network connectivity, hog bandwidth, turn company resources against itself, etc. A few options to consider when planning for this situation (and writing a policy) are properly configured router filters, TCP SYN flooding patches, disabling network services that are not used, and observing machine performance (create baselines for normal activity). (Carnegie Mellon University)

Social Engineering

Social engineering is a popular technique used to breach security that does not require a computer. There are many definitions to describe social engineering, most agreeing on one thing: gathering information that grants access to systems for malicious intent. Social engineering is similar to hacking, but it manipulates individual's trust to gain their information rather than manipulating company resources. This may be accomplished through several methods. One such

method is the telephone. Individuals may call and act like someone with "clout" within a company and simply say they have forgotten their password or can not gain access to a particular server or application. Help desks are extremely susceptible to this kind of attack. They are paid to answer questions and do not take the time to verify the identity of the caller. It is important here to add guidelines (within security policies and/or training programs) to verify identity when these calls (or any call) are made and information is requested. Another popular technique is known as dumpster diving. Individuals will actually go through company dumpsters or trashcans looking for valuable information that will help them gain access to systems. Items such as phone books, manuals, memos, charts, etc can serve as valuable information to a hacker. Phone books provide phone numbers of people to impersonate; manuals may give information about particular systems within the company, etc. Make sure to add a policy for destroying (shredding is good) any and all sensitive information. There are many other types of social engineering, such as on-line social engineering and simple persuasion that need to be guarded against. This is an issue that is typically overlooked. Make sure to outline, in detail, preventative measures against social engineering attacks. (Granger)

Inside threats

Users are among a very common but overlooked security threat. It has been argued that protecting from the inside is more important than the outside. While most incidents regarding end users are unintentional, they can still warrant a disastrous situation. End users tend to take advantage of certain Internet related "luxuries" that can open up holes in information systems. Chat rooms, games, real player, real audio, etc all open up certain ports for communication which can lead to an entry point for an intruder (hacker). End users also tend to write down user names and passwords and hide them under their keyboards, in their desks, or some other place easily accessible to other individuals. A good example here is a disgruntled employee who might go around after hours looking for this type of information. He/she might use it themselves or pass it on to a potential hacker. Addressing these issues in an end user training policy and/or an acceptable use policy can be implemented here to mitigate these risks. It is advisable to have employees sign off on acceptable use guidelines to make certain they are aware.

Natural disasters – Floods, Tornadoes, Fire, etc

Mother nature is also a real threat. Floods, tornadoes, fires, and earthquakes can become a disaster for a company. In the event that a disaster occurs, the best plan is to have a proven disaster recovery plan (discussed later) that has been tested over and over again. Within this plan should be a detailed section for conducting

backups of all critical systems and storing these backups at an off-site location that can be reached in a reasonable amount of time. There should also be a backup location (again, accessible in a reasonable amount of time and identified in the policy) where a company can implement the backups that have been stored off-site.

Identify Specific Policies

Two questions often arise when planning for a security policy. Should I implement one "blanket" policy or should I separate them into smaller, more specific policies? There is no particular right or wrong answer. Either approach is acceptable; just decide which one is best for the company. Regardless of which method is chosen, there are some core areas that should be considered in any security policy.

Internet Use

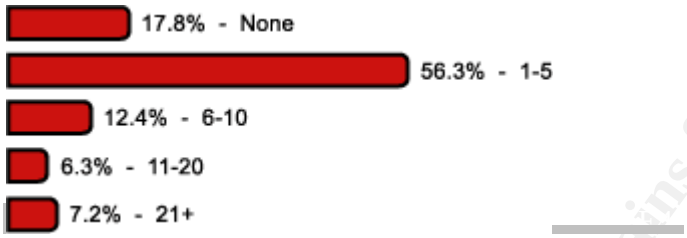
The Internet is among the most abused privilege in the workplace. Employees do everything from surfing, to gaming, to online shopping (among other things) during work hours. Personal email usage is also a big issue. Both can lead to legal ramifications. Without an Internet use policy, companies are at risk for litigation. Employees have a legitimate court case if they were terminated for conducting this type of activity if it was not stated as "prohibited" use in an Internet policy. In order to manage Internet use issues, there are a few things to consider. Create an Internet use policy outlining what is acceptable use and what is prohibited use. Also, list the times that acceptable use of the Internet (for personal use) is acceptable (during lunch, after/before regular work hours). Have employees read and sign the companies Internet use policy, and make it part of new employee orientation. It is also a good idea to add it to the end user training program. Take a look at a few survey results from Vault.com.

Web Surfing
During an average workday, how much time do you spend surfing non-work-related sites?

Source: Vault.com Internet Use Survey of 451 Employees, Fall 2000

E-mails Sent

On average, how many non-work-related e-mails do you send during the workday?



Source: Vault.com Internet Use Survey of 451 Employees, Fall 2000

Anti-Virus

As mentioned earlier, viruses are at an all time high in today's cyber community. While anti-virus software is definitely a must have, there must also be an anti-virus policy to accompany the software. First thing to do is to adopt a corporate standard anti-virus software package to write the policy around. Basic guidelines to consider in the policy are: never open mail from a suspicious or unknown source, delete junk mail upon receipt, avoid downloads from unfamiliar sources, scan diskettes, and demand periodic updates of anti-virus software from end users. Also, add a section requiring anti-virus software on all systems accessing the company network (remote access) from outside the company. (SANS Institute)

Disaster Recovery

Simply implementing a plan for recovering company data in the event of a disaster is a major accomplishment in disaster recovery. While natural disasters and viruses were mentioned earlier, there are many more incidents that can cripple a company. Data corruption, hard drive failures, power failures, data deletion, and theft are all possible scenarios that should be planned for. The best place to start planning for disaster recovery is in the every day business practices within the company. There are many questions to answer about the environment and a few basic practices that should be considered in a disaster recovery plan. Always use appropriate personnel when developing backup and restoration procedures. Also, test the procedures periodically. Make sure that data can be restored in a timely manner. Keep backup logs available for faster granular file restores. Employees also should be trained to backup other employees in the event that they are not able. Unfortunately, the tragedy of September 11 has shown us that when disaster

strikes, resources are not the only assets that can be lost. These are only a few standard practices to consider. While a whole paper can be written about disaster recovery, the main thing to learn here is to identify critical assets, back them up, and practice recovery procedures to be ready for a disaster. (BakBone Software)

Auditing

Auditing is a key function that must be performed in order to have a successful security program. Audits are key to learning internal communications patterns and then using that baseline as a guide to determine suspicious activity. Auditing is also a valuable forensics tool when learning about an attack. Administrators need to be able to trace steps to determine what was done to the system(s), what was taken, and/or what might have been replaced. Audits also provide information about end-users that may have obtained privileges (whether intentionally or unintentionally) that exceed their job needs. Audits also need to be performed on administrators (system, network, etc) to know what they accessed using their privileges and if they have performed suspicious or abnormal actions. A successful auditing policy should outline key personnel involved in audits, categorize company assets (critical, mission essential, etc), establish criterion for risks, prioritize identified risks, develop recommendations, etc. A section should also be created to outline the adopted tool sets used to audit systems.

Email

It is advisable to choose words wisely when creating an email use policy. End users tend to be reluctant in accepting email policies because they feel it infringes on their personal privacy. This is where management support plays another key role. Representatives from every pertinent office of an organization should be involved, such as executive management, IT department, human resources, and the legal department. Since employees feel the have the right to use email however they wish, it is important to train them on acceptable use and unacceptable use. Lets look at a few unacceptable issues. Web based email should be banned totally. Keeping viruses out the company is hard enough. Web based email leaves an organization further susceptible to viruses, inappropriate mail, and SPAM mail. Using email for pornographic or obscene use should definitely be prohibited. Abusive language to other employees or customers constitutes unacceptable use. Running a personal business through company email, or company resources for that matter, should also be prohibited. Defamation of company character is not only forbidden, but also bad for job security. Email filters may also be a consideration to add to an email policy (again, management and corporate lawyers should be consulted with before

implementing this). Certain file types that are known to have virus characteristics, such as .exe files and .vbs files, should be blocked. SPAM filters may also be considered to filter unsolicited mail as well as specific phrases within messages. To sum up email policies, involve corporate lawyers, stay committed to the policy, educate users, take advantage of email filters, and enforce all policies. (SurfControl)

Are you worried about your employer monitoring emails? 42% said yes

Vault.com - Email behavior in the workplace. May 2000

Password

Passwords serve as the first line of defense for user accounts. While passwords are a necessity, they are only as good as there strength. It is unwise to simply trust that employees (contractors included) are implementing strong passwords and changing them periodically. This is why a password policy should be implemented. The policy should state password length (more than 8 alphanumeric characters), require special characters (!@#$%&), require both upper and lower case characters, does not include personal information (family names, pet names, favorite football team), words not found in any dictionary of any language, and should be changed at least every six months. The policy should also state what users must not do. Prohibited activities should include never revealing passwords over the phone, never revealing passwords in emails or other documents, never talking about passwords in front of others, never writing down passwords and/or storing them, etc. Passwords may be the weakest link without an enforceable policy.

Remote Access

A remote access policy governs access to company networks from any host. Damages such as data loss, loss of sensitive company data, and damage to critical internal systems are a few of many risks that are involved in remote connections to company systems. The policy should not only apply to company owned machines (typically laptops), but to personal owned computers that connect to company resources. Every possible medium (modem, ISDN, DSL, etc) should be covered. Employees should treat remote access connections no differently than their "on-site" machines. That includes complying with all company policies even though the user is *typically* not in a company building. While remote access utilizes passwords, there may be other tools (public/private keys) used to authenticate, so it is important to list additional authentication requirements for

remote access. A requirement should also be added regarding connections to other networks. At no time should a machine utilizing remote access to use company resources be connected simultaneously to another network. In addition, all systems should be required to have the latest version of company approved anti-virus software. The above issues should serve as core requirements for a remote access policy. Certainly all companies are different, so additional requirements will likely need to be implemented. (SANS Institute)

Configuration Management

Configuration management also plays a key role in information security. One cannot protect what one does not know they have. Overlooked remote access connections could be taking place, an unknown server could be sitting in a room that is hardly used, or a new software package could have been implemented that poses security vulnerabilities. Configuration management provides a systematic way of keeping track of things such as this, which need to be protected. All hardware and software systems should be identified and any changes made must be documented. A few key elements to consider in the policy are identification, control, audit, and reporting. A labeling system should be created and outlined in the configuration management policy. Each piece of hardware (including pc's, servers, routers, appliance firewalls, etc) and software (including operating systems, ant-virus software, intrusion detection systems, etc) must be labeled for identification. While labeling hardware is self-explanatory, one should label software by name/vendor and version number. A method of controlling changes in hardware and software must also be outlined in the policy. Control must be established to keep resource inventory current. Compatibility problems and vulnerability threats would most definitely arise without control measures. Auditing comes into play and acts as a checks and balances system for configuration management procedures. Outline a routine audit procedure in the configuration management plan to make certain all assets are accounted for and changes have been documented. Reporting allows security, network, and system managers to evaluate configuration changes and trends over time. As it pertains to security, configuration management is a valuable tool in keeping track of company assets, which is obviously necessary in order to protect them from a potential security incident. (Allan)

Summary

Creating a security policy is difficult and is more complicated than simply writing a policy and putting it on the shelf. It is important to first define what a security policy means with regard to an organization, or in other words, how much security is needed? Next, justify the need to corporate management, as they are a vital key in this process. As mentioned

earlier, there may be some resistance, but be persistent. Persistency eventually pays off in this situation. Do not reinvent the wheel! If policies are in place, review them and make necessary changes before starting from scratch. It may save a little work. Identify and locate all assets. A security policy should be designed around the critical ones (assets) that are identified. An important next step is to identify threats to company assets. Identify which threats are critical and which ones are acceptable to the company. Next, decide if the policy will be one document or comprised of various, more specific policies. Either one is acceptable. Once the policy is written, or in a draft form with an outline, decide if the policy is clear, if it outlines responsibility, and if it is enforceable. It is better to find out now instead of after the policy has been completed and implemented. Also, do not forget about the legal department. They are there to keep the company out of trouble and need to be involved in the construction of this policy.

Security policies are only part of an effective security program. An effective security program is not event driven; it is a life cycle approach that calls for a continuous "hands and eyes" approach. Security personnel must be available to conduct periodic reviews, system scans, audits, and all require a person that has the ability to analyze and evaluate the data. A security program will only be successful if continuous risk reviews start the life cycle over again with management and legal approval that results in a review of policies and procedures, daily administration, and verification audits.

References

1) Winkler, Ira S. "Who are the Hackers?" URL: http://www.infowar.com/hacker/whohacks.html-ssi (31 Jan 2002).

2) Shaw, George. "Port Scanning Graphs." Hacking Information and Statistics. 18 Feb 2001. URL: http://www.btinternet.com/~shawweb/george/hacks/graphs.html (31 Jan 2002).

3) Shaw, George. "Hacking Graphs." Hacking Information and Statistics. 18 Feb 2001. URL: http://www.btinternet.com/~shawweb/george/hacks/graphs1.html (31 Jan 2002).

4) University of Vanderbilt. "Brief Introduction to Viruses, Trojans, and Worms." AntiVirus Information. URL: http://www.vanderbilt.edu/its/antivirus/AVInformation.html (31 Jan 2002).

5) Granger, Sarah. "Social Engineering Fundamentals, Part 1: Hacker Tactics." 18 Dec 2001. URL: http://online.securityfocus.com/infocus/1527 (31 Jan 2002).

6) Vault Inc. "Web Surfing." Results of Vault Survey of Internet Use in the Workplace. URL:

http://www.vault.com/surveys/internetuse2000/results2000.jsp?results=2&image=employee (1 Mar 2002).

7) Vault Inc. "Emails Sent." Results of Vault Survey of Internet Use in the Workplace. URL: http://www.vault.com/surveys/internetuse2000/results2000.jsp?results=4&image=employee (1 Mar 2002).

8) SANS Institute. "Guidelines on Anti-Virus Process." URL: http://www.sans.org/newlook/resources/policies/Anti-virus_Guidelines.pdf (4 Feb 2002).

9) BakBone Software. "Developing a Disaster Recovery Procedure with NetVault Backup Software." URL: http://www.storagesearch.com/bakboneart.html (4 Feb 2002).

10) SurfControl. "How to write an Email Acceptable Use Policy." The Manager's Email Guide. URL: http://www.surfcontrol.com/general/assets/whitepapers/how_to_write_an_email_aup_uk.pdf (20 Feb 2002).

11) SANS Institute. "Remote Access Policy." URL: http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.pdf (20 Feb 2002).

12) Allan, George W. "What is Configuration Management?" Logistics Spectrum, Vol. 31 No. 1: pp. 15-18, ISSN 0024-5852. 1997. URL: http://www.dis.port.ac.uk/~allangw/papers/pub97a.htm (20 Feb 2002).

13) Bounds, Nadine M., Dart, Susan. "The Beginning to your CM solution." 26 Nov 2001. URL: http://www.sei.cmu.edu/legacy/scm/papers/CM_Plans/CMPlans.MasterToC.html (28 Feb 2002).

14) Fraser, B. "Site Security Handbook." September 1997. URL: http://www.zvon.org/tmRFC/RFC2196/Output/chapter2.html (24 Feb 2002).

15) Security Complete. San Francisco: Cybex, 2001. 17–40.

16) Carnegie Mellon University. "Denial of Service Attacks." June 4, 2001. URL: http://www.cert.org/tech_tips/denial_of_service.html - history (24 Feb 2002).