A Vulnerability Management Approach

David C. French
March 7, 2004
GIAC GSEC Practical Assignment V 1.4b

Abstract

The purpose of this paper is to discuss the application of vulnerability management and the processes and technologies that make up this strategy. In this paper, areas of discussion will focus on the vulnerability lifecycle, the role vulnerability management can play, the approach to vulnerability management, tools to assist with the process, and reasons why such a process should be implemented in order to help mitigate network security risks.

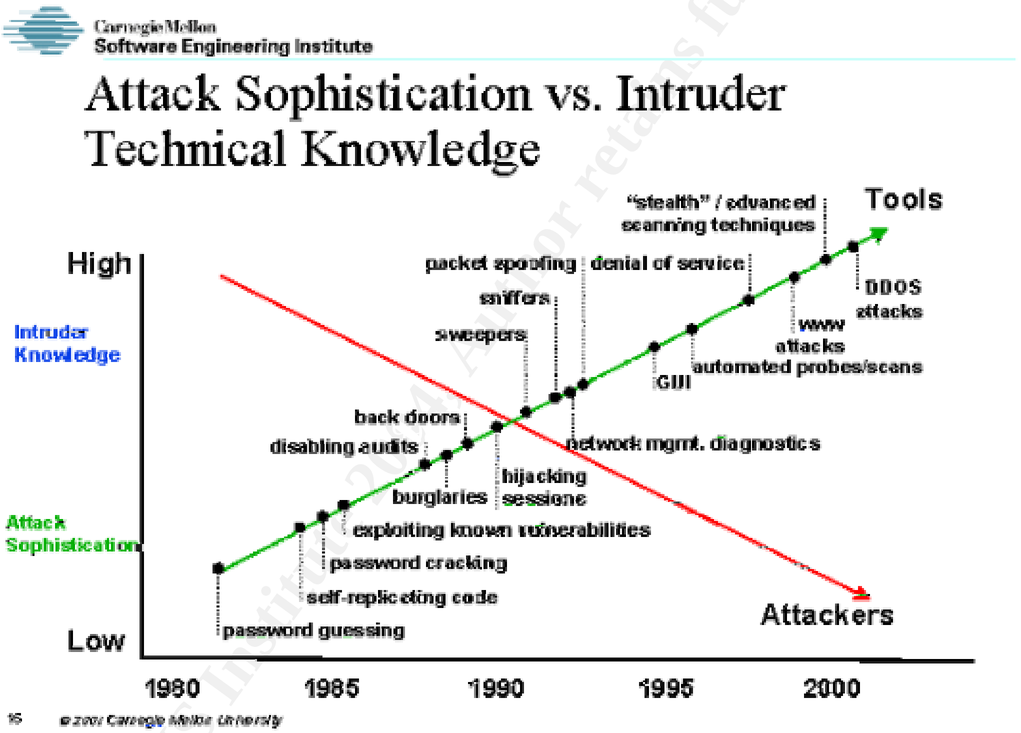
The number of vulnerabilities discovered and exposed has been on the rise throughout the past ten years. The number of incidents reported has risen exponentially in one year alone, from 82094 in 2002 to 137529 in 2003 according to statistics drawn from the CERT Coordination Center. As the potential for exploitation has increased, solutions have become in high demand to help deter and minimize the effects of such potential risks. For instance, organizations began installing network protective devices such as firewalls, and could gain a reasonable feeling of assurance to know that their systems are more secure because this technology. Critical systems are protected by the firewall, and IDS systems adequately detect and thwart potential intruders.

Firewalls, IDS systems, and anti-virus will not fully protect corporate networks from attack. Because of the way technology has changed and evolved, vulnerabilities are also becoming increasingly complex. For instance, web application hacking has become a very popular technique used to subvert corporate and other private networks. By hacking the web application, an intruder is attacking a function in which corporations must permit into their networks in order to do business. Companies need to allow this type of traffic, thus, increasing the risk.

In this paper, we will discuss some of the proactive steps in the vulnerability management to enable companies to stay ahead of the curve. We will point out specific technologies that may be utilized as part of the process to automate vulnerability and asset management. We will also discuss a few other practices that should be incorporated into the corporate security strategy, such as secure coding and security awareness.

The Vulnerability Lifecycle

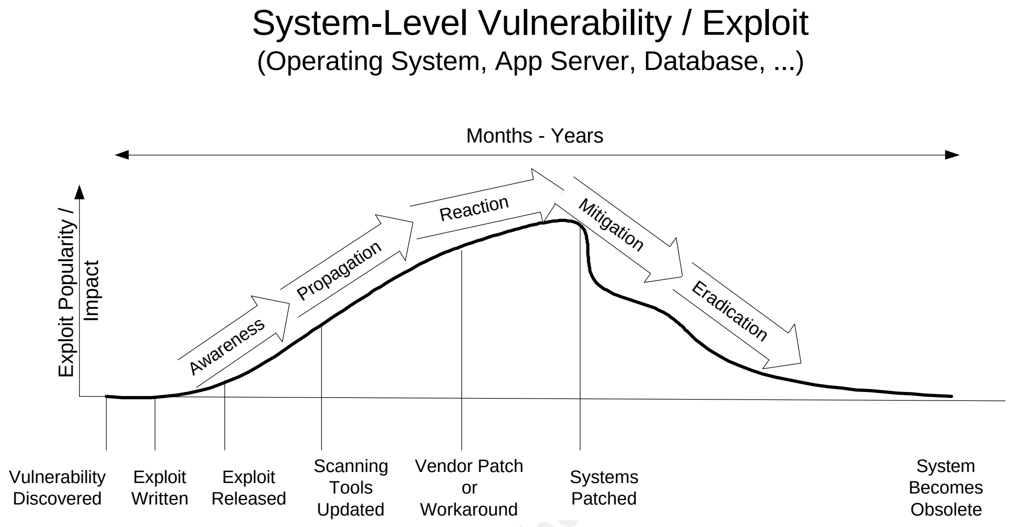
Hacker sophistication is constantly changing along side the advancement and deployment of new technologies. In the early stages of the Internet, hacking consisted of simple password guessing attacks and deployment of self-replicating code. Attacks then became cleverer, adding back doors, disabling auditing, sniffing, session hijacking, and distributed denial of service attacks. And lately, the sophistication has matured to very complex web application attacks involving the likes of cross-site scripting, SQL injection, and other backend database hacking techniques. Unbelievably, with this advancement in sophistication comes the ease of the execution of these attacks. Automated tools and exploit code enable intruders with a relatively low level of knowledge to exploit vulnerabilities at will, and on a large scale. To observe this graphically, please see the following diagram:



(Pethia)

With this in mind, you can now draw a picture in your mind of what the vulnerability life cycle might look like once a vulnerability is discovered. Take for instance one of the critical Microsoft vulnerabilities that had been exposed over the past few years, the MS SQL slammer worm. CERT received reports of the MS SQL "slammer" worm propagating last January 2003 (CERT). Therefore, around that time, code was released that exploited a vulnerability in the Microsoft SQL with instructions to spread itself all over the internet, probing and attacking other vulnerable servers. However, some of the root causes of the vulnerabilities exploited by this worm were actually discovered and made public in July 2002 (CERT), six months before the worm was actually distributed into the wild.

Therefore, had network and system administrators been aware of the patches that had become available from Microsoft, and promptly tested and deployed these patches to alleviate the vulnerability, the worm may have not spread so quickly and caused so much technological and financial damage. This theory can be graphically depicted in the following diagram:



(Lipson)

Vulnerability Management

It is critical for all organizations, regardless of size to be able to identify, prioritize and mitigate security risks in an effective manner. It is often difficult to quantify the ROI for implementing and such plans where there is no direct, positive impact on the financial bottom line. However, it is possible to quantify the costs of a customer not being able to access your web site to complete a purchase transaction, or a business partner who's electronic transaction becomes halted due to a denial of service attack on your systems. For instance, according to the 2003 CSI/FBI Computer Crime and Security Survey, $70,195,900 is the dollar amount that was lost due to theft of proprietary information, and $65,643,300 was lost due to denial of service attacks.   "And yet, despite the documented costs of cyber attacks by hackers, viruses – even trusted employees within organizations – the security posture in most large enterprises is still characterized by a series of largely disconnected measures and countermeasures designed to respond to events after they have occurred. Current security strategies are, in other words, reactive in nature – not proactive" (CRA Reports). As an information security consultant, I continuously encounter medium to large size companies that have little, if not any [proactive vulnerability management procedures in place.

In order to implement an effective vulnerability management plan and achieve success, three aspects must be kept in mind; a comprehensive approach, technology, and trained people.

There are many different approaches that have been researched and developed by security firms and research and development organizations. For example, consulting firms have developed solutions to help organizations create a strategic vision, and develop areas such as vulnerability management programs and secure network architectures. Technology companies have developed product solutions to aid with the automation of vulnerability assessment procedures. The CERT Coordination Center at Carnegie Mellon University has come up with the CERT OCTAVE approach, which is highly regarded in the industry. In this section, I'm going to outline, at a high level, a logical approach to vulnerability management, drawing strengths from various approaches.

First, a vulnerability management team must be established. This team should consist of all individuals that have a vested interest in the security of information and networked systems. For instance, system owners should be involved in the vulnerability management process. Because changes and updates will be consistently applied to systems, proper approvals from system owners must be attained through the corporate change management process. Systems administrators and information security staff will be responsible for identifying risks and implementing remediation procedures. Information security management will be responsible for monitoring the process to ensure productivity and success.

Next, policies should be developed and adhered to throughout the ongoing vulnerability management process. Policies and procedures will lay the groundwork and help information security attain the necessary buy-in across the organization. In many organizations I've worked with, there is an absence of a central source of information and procedures on how to go about vulnerability management in a consistent manner. Policies supply a framework and structure, providing a centralized point of guidance for employees to follow consistent processes throughout the organization.

The next critical step is to perform a complete asset inventory of the corporate network. Discovery of all computing resources that reside on the network must be completed, including all servers, PC's, network devices, operating systems, applications, etc. During this process, you will attain a good understanding of the defensive tools your organization may already have in place; for instance, firewalls, intrusion detection systems, anti-virus, and vulnerability scanners. Throughout the asset inventory process, it is very important to keep in mind the business processes that your systems impact. This is the main reason you are performing this step in order to identify the most critical systems on your network. "Once the mapping is complete, we can prioritize security measures on the basis of aggregate potential losses for groups of assets that map to securable entities such as local area network segments, media or business units" (Barwise).

In order to perform an asset inventory, automated tools and scanners should be leveraged. For instance, there are several types of port scanning and vulnerability assessment tools available for free or commercial use:

- GFI Languard Network Security Scanner– Freeware and commercial versions. This tool may be used for discovery and vulnerability scanning, and provides a reporting mechanism. Reports may be generated into easily readable XML files.

- Nessus Security Scanner – Freeware tool. Enables you to scan entire network ranges utilizing a distributed type of approach. For instance, you can run a Nessus client on your laptop, and connect to different instances of a Nessus Server that you may install on a UNIX based systems. You can configure and run scans on the UNIX Nessus server from your Windows based client. Reporting capability: reports may be generated into HTML, Adobe Acrobat, or plain text files.

- Retina Security Scanner – Commercial network vulnerability scanner. This scanner enables you to scan network segments and inventory and identify vulnerabilities.

- ISS Security Scanner – Commercial network vulnerability and discovery scanner with robust reporting capabilities.

Later in this paper, I will discuss some next generation tools that incorporate the function of vulnerability scanners within an all inclusive vulnerability management solution.

Once you have identified all of the systems that reside on your network, it is essential to prioritize these assets. The objective of prioritizing is to determine what assets have the greatest effect on how your organization does business. What systems must always function with no interruptions? What applications are most critical, and what systems and network segments do these applications rely upon? Questions like these will help prioritize assets to focus on immediately.

Now, the next step is to assess all of the information you have obtained for your most critical systems and applications as a result of the discovery and vulnerability scanning procedures. What vulnerabilities seem to have the highest risk and might have the greatest impact on your systems? Are these vulnerabilities potentially exploitable on your critical systems and applications? Do compensating controls exist on the network? After all, there may be a laundry list of potential high-risk vulnerabilities, however, which possess the most imminent threat? This can all depend on a number of factors such as where the systems are located, accessibility from the public Internet, compensating controls that may already be in place, etc. All of these factors and more need to be considered and discussed amongst the vulnerability management team.

There are many sources of information available to help your team manage and assess all of this overwhelming information. Organizations like the CERT Coordination Center, SANS and the Computer Security Institute are central sources of information for security professionals to reference.

Calculating Risk

Through my research, I have found much debate over how to calculate risk and what information is used to derive a risk rating. Vulnerability characteristics must be considered, along with the value of the assets you are trying to determine a risk ranking for. Risk rankings and classifications may vary by operating system, threat of the vulnerability, probability, business functions impacted, and other significant values depending on the organization.

Once all of your information is collected, you can incorporate the identified variables to formulate a risk model based on your organization. One example is the following model derived from the research of the Washington Bureau of CRA Reports:

Risk = Asset Value x Vulnerability x Threat

Utilizing an appropriate model can help organizations determine what vulnerabilities might have the highest impact and on what areas of the business. “A vulnerability only becomes an issue for your organization when it actually presents a threat” (TruSecure).

Patch Management

Now that we have identified areas of risk and the criticality of assets, risk remediation procedures must be employed. One example of a risk remediation effort is patch management. Much like the vulnerability management process, patch management is a team effort, and will involve all parties with a vested interest in security. “Effective patch management, one means of dealing with these increasing security threats, includes several critical elements, such as top management support, standardized policies, dedicated resources, risk assessment, and testing” (Dacey). As mentioned before, system owners will need to be involved throughout the change management process. Systems administrators and network security administrators will need to be involved to test and successfully deploy technological changes and enhancements to alleviate the threat of vulnerabilities.

Testing must be built into the policies and procedures that you have already established within your vulnerability management plan, and should always be performed before rolling out to production. This will help prevent the risk of inadvertently affecting other business functions as a result of applying system patches. Before changes are implemented into production, system owners should authorize proper approvals, and all maintenance policies should be adhered to. Some circumstances will warrant immediate deployment depending on risk and asset criticality, however, testing procedures should be employed to the fullest extent possible.

Continuous Enhancement

"According to the most recent CSI/FBI cybercrime study, over 90% of reported cybercrime attacks take advantage of known vulnerabilities – vulnerabilities that were identified before the actual attack" (TruSecure). This is why it is so important to employ an effective vulnerability management program. More importantly, it is important to maintain and monitor a successful practice, and to continually assess and improve the vulnerability management process as your environment changes. "Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected" (Brock). Vulnerability management must become part of your staff's job description, across all levels involved. Members of your team must be held accountable for their part of the process, and must be actively involved in its continued success. "The impact of the entire system on both the security posture of the organization, as well as on the use of security and technical resources should be watched closely with an eye for finding areas of improvement (CRA Reports).

Is Help Available?

Vulnerability management and process deployment can become quite overwhelming for information security leadership. Deploying a centralized and focused vulnerability management plan can be difficult, especially when dealing with geographically separated teams and decentralized computing facilities. Challenges are presented with maintaining documentation, communication, change management, reporting, etc. However, the information security industry has responded to the ever increasing needs for vulnerability management solutions, and there are choices available to help make the process more efficient, effective, and easier to manage.

Solutions have been created that enable organizations to execute vulnerability management strategies within an automated and centralized environment. These tools allow for the automated scanning and discovery of all networked systems, and real-time vulnerability alerting capabilities. They enable the tracking of vulnerability remediation activities and the assignment of remediation tasks. In addition, it is possible to keep track of system configuration changes. This is an essential capability because vulnerabilities continuously surface in real time and may take affect with addition of new software or networked services. Most importantly, these types of next-generation vulnerability management tools also give organizations the ability to centrally deploy vulnerability management processes, to maintain a central point of reference for information resources, and to assign values to assets based on prioritization. "An "asset-based" system – one that assigns value to specific assets based on how important they are to your organization's core business – allows you to make a much more accurate risk determination" (TruSecure).

There are many vendors that provide vulnerability management solutions, but you'll need to ensure your organization chooses the one that makes the most sense and best fits your infrastructure's requirements. I've conducted research on vulnerability management vendors including Bindview, InteractNetworks, Computer Associates, and Qualys. Specifically, I'd like to describe some of the features that make up vulnerability management tools, and convey how they might provide an automated and centralized point of execution.

Vulnerability Management Tool Solution

Vulnerability management tools allow for safe and secure access through a web interface over the encrypted HTTPS protocol. Unique user accounts may be created for system administrators, network security personnel, managers, and whoever has a vested interest and responsibility for executing a vulnerability management strategy.

The following are valuable features of vulnerability management tools:

- Real-time/hourly vulnerability alerting and updating
- Auto-discovery scheduling – the tool will perform discovery on an established time schedule to provide continuous asset inventory
- Asset profile creation and modification through web management interface
- On-demand vulnerability assessment
- Reporting capability by vulnerability, asset, configuration standards, SANS top 20 vulnerability lists, and audit reporting
- Web services infrastructure for global deployment and reporting functionality
- Asset prioritization and risk ranking model
- Configuration standard capabilities – Organizations may create standard configuration settings based on assets managed
- Task completion tracking – tasks may be assigned to responsible system owners and administrators to apply security patches, and the tool will track activity and task status
- Support for all Windows and UNIX based operating systems; Windows 2000/XP/2003, NT, UNIX AIX, HP-UX, Sun Solaris, Red Hat Linux

However, as previously mentioned, a single tool will not adequately give you an effective vulnerability management process. Skilled people play a vital role in the vulnerability management process, and it is essential to provide adequate training and security awareness to your staff.

Are there other good reasons to invoke a proactive vulnerability management process as part of your strategic security initiative? What about shareholder value, or compliance to formal standards and Government regulations?

Government Regulations

"For a growing number of companies, emerging government regulations at the federal, state and local levels are further prompting a more strategic approach to managing risk" (CRA Reports). As such, vulnerability management programs are going to play a significant role in strategic security plans, and corporations are going to need to bring processes up to speed in order to satisfy such regulatory requirements. Specific government regulations and standards that have sparked such attention are as follows:

- Gramm-Leach-Bliley Act
- California's SB 1386
- HIPPA – The Health Insurance Portability and Accountability Act
- Sarbanes-Oxley Act
- ISO 17799

These regulations call on organizations such as financial service, hospitals, and all public companies to improve upon information security. An important way in which to satisfy such requirements is through the development of comprehensive and consistent vulnerability management processes.

There is another area of particular interest regarding information security that has generated a lot of attention recently, and is a reason for the growing number of incidents being reported; secure coding practices.

Secure Coding Practices

I mentioned in the beginning of this paper that with the emergence of new and innovative technologies, new techniques have surfaces to exploit potential weaknesses. Specifically, it is necessary to address the emergence of web application hacking, which has become quite an issue for IT organizations.

In addition to the traditional HTML coding language, which facilitates a static, non-interactive functionality, new and robust languages have been developed to improve web site capabilities. These new programming languages have enabling organizations to create interactive, robust, and highly functional web sites. For instance, XML, PHP, and Java are three such languages that have become quite popular. Because of these new developments, companies have enabled communication directly with consumers and business partners over the public Internet through web enabled platforms based on a range of technologies. For example, Microsoft web sites are built using the ASP and .NET programming platforms. Many UNIX based web platforms such as Apache take advantage of Java and PHP.

However, problems have surfaced with the widespread use of these new technologies. Curious minds have figured out ways to essentially re-engineer web applications and the way web sites have been developed, enabling exploitation of inherent vulnerabilities that actually reside within the code itself. "Between 1995 and the first half of 2003, the CERT Coordination Center reported 11,555 security vulnerabilities that resulted from software flaws" (Dacey).

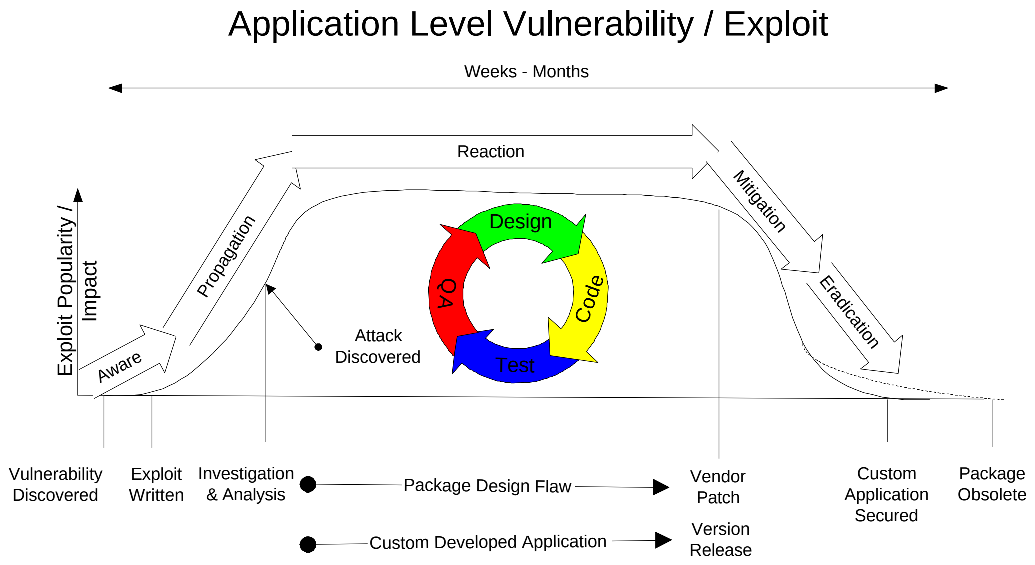
With that said, there has been an increasing pressure on software vendors to re-evaluate the processes that have been put into place for code review and quality assurance. An excessive number of vulnerabilities have been discovered and exploited within web application and software programs, and the demand for more secure products has influenced the need for a higher level of quality. Companies such as Microsoft have taken on new initiatives to promote secure coding practices within the software development process.

But not all software vulnerabilities are attributed to vendor software development. The methods that have been put into place by corporations to develop interactive code within their web applications to conduct business and make information publicly accessible to customers also contributes to the insecurities of web applications. "Security vulnerabilities found in the web application layer can be just as devastating as any other IT security threat; they can result in the loss of data confidentiality and integrity, while potentially leading to server, database and even network-level compromise" (Hemler, Nairn, Rollins). Developers, whether internal to a corporation or a third party vendor, are not following secure coding guidelines while developing web-enabled applications.

Vulnerabilities that may be exploited because of poor programming standards are attributed to the absence of proper user input validation checking. Examples include SQL injection, parameter tampering, and cross-site scripting. Other programming errors include hard coding username and password combinations, utilizing weak homegrown authentication schemes, and enabling insecure sample code. Web application vulnerabilities typically result in exploitation of back-end databases that contain sensitive information such as customer account information or business partner information. However, exploitation of such threats may be prevented if secure coding procedures are built into the development process and throughout all stages of the application development lifecycle.

Application Exploit Lifecycle

The application exploit lifecycle is very similar in theory to the system vulnerability exploit lifecycle discussed earlier in this paper. However, in the following diagram, the idea is conveyed in relation to the phases of the application development lifecycle:



(Lipson) leveraged information

This example shows different points at which a vulnerability may surface and have an impact on the application development lifecycle.

Therefore, secure coding practices must be adhered to throughout the entire lifecycle of application development and maintenance. Reviewing code for security vulnerabilities during the development phase is crucial to catching coding errors that may result in significant vulnerabilities in the long run. It is also cost beneficial to catch potential errors within early stages, as problems may cost a significant amount of money to remedy once the application is completely deployed into production. More critically, potential losses may be insurmountable if vulnerabilities are actually exploited by unauthorized individuals with criminal or malicious intent. In addition, by implementing secure coding practices during the development phase, programmers are able to understand how they inadvertently caused a potential vulnerability, and will be more inclined not to make the same mistake in the future.

Throughout the life of the application, it is a highly beneficial to perform periodic application security reviews of your web-enabled applications. With the continuous updating and enhancing of web application code, there is the risk of inadvertent introduction of new security vulnerabilities. By testing for vulnerabilities on a periodic basis, organizations can help ensure that secure coding procedures are being followed, and where exceptions occur, implement proper remediation steps.

Summary

As discussed throughout this paper, there are several aspects that must be considered in order to successfully deploy and maintain an effective vulnerability management process. Among the most important are skilled people, a comprehensive approach, and enabling technology. Organizations must begin instituting vulnerability management plans to uphold security standards and comply with certain regulatory pressures, and to maintain shareholder trust and market share. There are many technological solutions available to help automate and effectively deploy a vulnerability management process. However, it is critical that asset and risk prioritization be at the forefront of every plan in order to effectively focus on the most important areas of potential risk to the business. By pulling together the essential elements such as trained people, a comprehensive process, and enabling technology, organizations will work towards a proactive state of security.

References

Pethia, Rich. “Internet Security Trends.” Software Engineering Institute, Carnegie Mellon University. 16 Feb. 2001.
URL: http://www.cert.org/present/internet-security-trends/sld001.htm (5 Feb. 2004)

Barwise, Mark. “Calculating the risk equation.” Computer Weekly. 16 January 2003.
URL: http://www.computerweekly.com/Article118681.htm (1 Feb. 2004)

“The Next Generation of Threat Management.” TruSecure Corporation. 26 Jan. 2004
URL: http://wp.bitpipe.com/resource/org_976306006_48/Trusecurewp_Threat-Management.pdf (5 Feb. 2004)

Lipson, Howard F, Ph. D. “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.” CERT Coordination Center. Nov. 2002
URL: http://www.cert.org/archive/pdf/02sr009.pdf (1 Feb 2004)

Dacey, Robert F. “Effective Patch Management is Critical to Mitigating Software Vulnerabilities.” US General Accounting Office (GAO). 10 Sep. 2003
URL: http://www.intellnet.org/documents/1200/080/1280.pdf (1 Feb. 2004)

“Security Risk Management: Strategies for Managing Vulnerabilities and Threats to Critical Digital Assets.” CRA Reports. Copyright 2003
URL: http://www.foundstone.com/pdf/security_risk_management.pdf (1 Feb. 2004)

“CSI/FBI Computer Crime and Security Survey.” Computer Security Institute. Copyright 2003. URL: http://www.gocsi.com/forms/fbi/pdf.jhtml (5 Feb. 2004)

Hemler, Joseph., Nairn, Andrew., Rollins, Kerry. “What’s in Your Web Root?” Ernst & Young LLP. 2004.

Brock, Jack L. “Information Security Risk Assessment, Practices of Leading Organizations.” US General Accounting Office (GAO). Nov. 1999
URL: http://www.gao.gov/special.pubs/ai00033.pdf (1 Feb. 2004)

CERT Advisory Referencing:
“CERT Advisory CA-2003-04 MS-SQL Server Worm.” CERT Coordination Center. 25 Jan. 2003.
URL: http://www.cert.org/advisories/CA-2003-04.html (1 Feb. 2004)

“CERT Advisory CA-2002-22 Multiple Vulnerabilities in Microsoft SQL Server.” CERT Coordination Center. 29 July 2002.
URL: http://www.cert.org/advisories/CA-2002-22.html (1 Feb 2004)