Global Information Assurance Certification Paper

CYBERSECURITY: LOOKING INWARD
INTERNAL THREAT EVALUATION

John M. Conte

May 22, 2003

GIAC Security Essentials Certification (GSEC)

Practical Assignment Version 1.4b.

Abstract

Computers have become an integral part of modern life. In the post 9-11 world, heightened computer network security efforts, focused on external and terrorist threats, should also address the threat posed from internal sources. Computer security threat evaluation must involve scrutiny of "insiders", those employees and business associates with system access within the protected perimeter of the network. An effective computer risk management program consists of risk assessment, risk mitigation, and evaluation and assessment by the organization. Insiders can pose many risks for an organization, some intentional and some inadvertent. Many risks might not ordinarily be perceived prior to problems arising. An insider accessing pornographic Internet sites using company equipment is an example of this. Pirated software appearing on company systems is another. Downloading copyrighted music from the Internet, inappropriate emails, theft of company information, bypassing firewalls to gain network access from outside, and inadvertent disclosure of company security information are other examples of potential risks.

Responses to these risks include limiting internal access and trust relationships on system networks, use of firewalls to shield critical functions, maintaining logs to identify internal users, limiting access to physical facilities, and implementation of internal intrusion detection systems. The most important factors might be careful screening of employees and outsiders allowed access to the network as well as active monitoring and evaluation of system activities.

Definition of Cybersecurity

"Much of modern life depends on computers and computer networks." (Computer Science and Telecommunications Board, p.2) Government and private enterprise employ computers and computer networks in critical and enterprise-wide operational and managerial functions. These applications include electronic communications, data processing, information storage and retrieval, and connectivity to other networked computer systems as well as the global World Wide Web (Internet). As more and more aspects of daily business activity are intertwined with computers and computer networks, issues of a system's integrity, reliability and security become more pronounced. In the post September 11th (2001) world, genuine concern has been manifested as to the ability and desire of anti-American and anti-Western fanatical political organizations and governments to attack and disrupt American government and business computer networks. It has become axiomatic that such threats are real and growing. (Verton)

While these global computer security concerns are paramount in the public consciousness, leaders of private enterprise and computer security professionals should focus on the more likely security breach scenarios posed by insider threats. Threats caused by an insider can be manifested in a variety of ways. An insider can provide system/network access to outsiders or an insider can engage in deliberate mischief or malicious activities within his or her own

area of trust. “Insiders” can be company employees, leased employees working for outside companies (sometimes referred to as externals), or vendors supplying computer or network products for insider use and who have insider access. Any unauthorized or non-business insider activities can cause significant problems for private enterprise.

Problems arising in a computer system or network can be classified as accidental or deliberate. Accidental causes can be sub classified as natural or “human but nondeliberate.” (Computer Science and Telecommunications Board, p.3) Deliberate causes are intentional malicious human acts. “Security experts often refer to the efforts of these malicious people as ‘attacks’. A central challenge in responding to an information system attack is identifying who the attacker is and distinguishing whether the motive is mischief, terrorism, or attack on the nation.” (Computer Science and Telecommunications Board, p.4)

With regard to cybersecurity, “[a] *vulnerability* is an error or a weakness in the design, implementation, or operation of a system. A *threat* is an adversary that is motivated to exploit a system vulnerability and is capable of doing so. *Risk* refers to the likelihood that a vulnerability will be exploited, or that a threat may become harmful.” (Computer Science and Telecommunications Board, p.6)

Cybersecurity can thus be thought of as a process whereby en evaluation is made as to what system vulnerabilities exist, which threats (people) might exploit these vulnerabilities, the likelihood that such threats will exploit these vulnerabilities, and a response plan to address these possibilities.

Computer Security Risk Management

“An effective risk management process is an important component of a successful IT [information technology] security program. The principal goal of an organization’s risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.” (National Institute of Standards and Technology, p.1)

Risk management involves risk assessment, risk mitigation, and evaluation and assessment by the organization. Risk assessment is the initial phase of risk management and is used to determine the scope of any potential threat. It can be subdivided into nine steps:

Step One - System Characterization. Identifies the boundaries of the IT system and its component resources and information.

Step Two - Threat Identification. Identifies potential threats and their sources that can exploit weaknesses (vulnerabilities).

Step Three - Vulnerability Identification. Identifies system flaws and weaknesses that could be exploited.

Step Four - Control Analysis. Analyzes controls currently in place, or contemplated for future use to address threats to known vulnerabilities.

Step Five - Likelihood Determination. Rates the probability that a specific vulnerability will be exploited by a potential threat in light of existing controls.

Step Six - Impact Analysis. Determines "the adverse impact resulting from a successful threat exercise of a vulnerability." (National Institute of Standards and Technology, p. 8)

Step Seven - Risk Determination. Assesses the overall level of risk to the subject IT system, i.e., the likelihood that a particular vulnerability will be exploited by a specific threat, its impact on the organization, and the degree to which controls reduced or eliminated the risk.

Step Eight - Control Recommendations. Recommendations to reduce or eliminate identified risks.

Step Nine - Results Documentation. Consists of the documentation of specific risk assessment results and recommendations by means of a risk assessment report or briefing. . (National Institute of Standards and Technology, p. 8-26)

Risk mitigation "involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process." (National Institute of Standards and Technology, p. 27) Risk mitigation can be achieved through:

1. Risk assumption (continue the function, possibly with risk reduction controls);
2. Risk avoidance (discontinue the function);
3. Risk limitation (implement controls to minimize impact);
4. Risk planning (risk mitigation planning);
5. Research and acknowledgment (admitting vulnerability and seeking controls); and
6. Risk transference (e.g., buying insurance). (National Institute of Standards and Technology, p.27)

Evaluation and assessment encompasses changes necessitated by the expansion and updating of network components, hardware and software, and personnel and security policy changes that result in new or resurrected risks.

Internal Threat Analysis

"INTENTIONAL ACTS OF EMPLOYEES are incidents like: Applications Program Change, Data Alteration, Data Denial, Disgruntled Employee Access, Embezzlement, Fraud, Fraudulent Data Entry, Hardware Denial, Hardware Alteration, Misuse of Resources, Operating System Penetration, Operating System Alteration, Privacy Act Violation, Software Denial, Strike, Unauthorized Disclosure. These threats are usually made manifest by employees who by deliberate, willful, or malicious intent destroy, divert, or improperly modify assets belonging to or controlled by their employer or host. Their actions may not always be illegal, as in the case of a strike, but they are unauthorized and harmful to the employer." (Carroll, p.55)

The subject matter literature commentary differs as to the extent of the internal threat faced by private enterprise with regard to computers and computer

networks. Some sources opine that the “vast majority of attacks originate from within an organization ….,”(Brenton, p.6) and that “[s]tatistics from the FBI Crime Lab consistently show that the majority of computer crime occurs from the inside.” (Escamilla, p.182) Another view holds that the insider attack problem is being overtaken by outsider attacks. A study conducted under the auspices of the FBI and the Computer Security Institute (CSI), in 1999, revealed “that *nearly half* of all such attacks started from *within the enterprise.* In previous years this annual survey has, in fact, indicated that *most* attacks were the result of an ‘inside job.’”(Crume, pp.88-87) One source, InterGov (www.integov.org), indicates that approximately eighty percent of computer and Internet-related crimes are perpetuated by insiders, with each episode costing business more than one hundred thousand dollars. (Carr) Another source, the Computer Security Institute (www.gocsi,com), indicates that insider unauthorized access accounts for more than seventy percent of all such activity. (Netvision) This threat has become so serious that "[t]he U.S. Secret Service, in conjunction with Carnegie Mellon University in Pittsburgh, has launched a study of insider-based computer security breaches that it hopes will ultimately help IT executives protect their systems from these attacks."(Gaudin)

Insider attacks can come from a disgruntled employee or a former employee. They can come from an outsider, assisted by an insider. They can originate from an external having insider access, such as a leased employee or a vendor. An internal user can obtain privileges belonging to other users, or attain administrator (root) authorization. In addition to privilege escalation, an insider can launch an attack against the network that would be blocked if initiated externally. An insider can be a hacker seeking to exploit the organization’s network for revenge, personal satisfaction, or a corporate spy seeking to obtain information or access for personal financial gain.

Insiders have advantages over external hackers. They “know which systems contain mission-critical data and which ones don’t; [they] know the company’s security policy and where it might be weak; [they] know the undocumented realities of how other employees may not actually adhere to the company’s security policy (e.g. shared passwords that are never changed); [they] have physical access to critical servers; [and they] are inside the perimeter firewall and, therefore, beyond its scope of control.”(Crume, p.88)

One of the growing problems created by insiders concerns the use and abuse of the Internet accessed through company networks. Respondents to the 2002 Computer Crime and Security Survey, conducted by the Computer Security Institute (CSI), reported that “[s]eventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).” (Computer Security Institute)

Offensive content

The accessing of sites containing images that might be pornographic exposes the company to potential liability from several sources. Accessing and saving pornographic images (however defined) can be a violation of the

company's internal employee code of conduct as well as privacy and Internet use policies. (Wiley Rein & Fielding, February, 2003) Employees not interested in this material can complain about a hostile work environment if they see or hear about these images in the workplace. Employees accessing, viewing or storing child pornography (defined by federal and state laws) on company equipment can be in violation of federal and local criminal statutes. This possession can trigger an affirmative duty to report and turn over this material to law enforcement authorities. As the law develops on criminal liability for Internet Providers, the day may come when IP's have to monitor third-party content, thereby creating additional opportunity for law enforcement to investigate child pornography accessed through the company network. (Waggoner)

Federal law, codified in the United States Code at Title 18, sections 2252, 2252(a), and 2260(b), prohibits, among other things, the simple possession of child pornography (as defined in these sections), including computer images. An affirmative defense (one that can be asserted even if the charge is true) found in these sections provides that if less than three such matters (child pornography) are in the possession of a person, that person can promptly and in good faith take steps to reasonably destroy these images without retaining them or allowing any other person to view them, except law enforcement. In the alternative, the person in possession of these images can report this information to law enforcement and must allow law enforcement access to these images. (Shannon, p.23)

This law is highly problematic for private enterprise. Mere "possession" of child pornography on a company network obligates that enterprise to remove it from the system or to notify law enforcement of its presence. There is no innocent possessor provision in the law (law enforcement excluded), other than the affirmative defense discussed above. Once suspected child pornography is discovered on a company system, that enterprise should actively work to delete it from all areas throughout the network. This creates a duty to act unlike the existence of adult pornography. In essence, child pornography that is intentionally or mistakenly taken into a company computer or network requires the possessor (the owner of the system) to actively remove and destroy all of the material. This process dictates creation and implementation of policies and procedures to check for the presence of child pornography on the network; to investigate the content, scope and source of this material; measures to remove and delete these items from anywhere present within the company; and a conscious decision whether or not to report this discovery to a law enforcement agency. These considerations have made the existence of suspected child pornography on company computers a big problem for business.

Additionally, local and state laws can also speak to the possession of child pornography on computers. (Bickel) An example of which is the South Carolina statute, Title 16, Section 16-3-850, that requires a film processor or computer technician to report (to law enforcement) film or computer images that contain sexually explicit pictures of minors. (Swanson)

Pirated software

The use of pirated software is another area of potential exposure for private business. The Business Software Alliance (BSA) a watchdog group, recently "announced that four New York area companies agreed to pay a combined total of $222,000 to settle claims relating to unlicensed copies of software programs installed on office computers." (Naraine) Action undertaken by BSA has resulted in more than $60 million in fines levied against companies' possession and use of pirated software. (Fisher) Audits conducted by BSA look for businesses that have insufficient licenses for the total number of actual users of a licensed product. (Kennedy)

Copyright infringement

The downloading of music from the Internet is another area of possible liability. It is illegal to make unauthorized copies of commercial music. Employees who copy protected recordings onto company equipment or distribute illegally copied music within a company network can open the company to legal action. (Allen)

Inappropriate e-mail

Inappropriate use of email, internally or externally, can be a source of problems if the recipient or unintended reader construes messages and attachments to be harassing, stalking, defamatory or obscene.

Theft of information

Internal and "external" employees who either intentionally or inadvertently export company information outside the internal security framework pose another area of insider threats. This might come about as a result of sending sensitive and confidential information to a home or offsite workstation, or a school or outside company server, to be accessed during non-work hours. Once information is imported on to an unsecured location it can be readily accessed by outsiders using the personal or vendor workstation or accessed by outsiders conducting Internet searches.

Security breaches

In an attempt to circumvent company security protocols in order to facilitate easy access to a workstation from a remote location, insiders sometimes utilize Internet connections that allow company firewalls to be bypassed. Perhaps without thinking about the consequences, this action can open a hole in the company's security apparatus. Periodic searches must be conducted to look for these go around connections.

Inadvertent disclosure

A more subtle breach of security by insiders encompasses information divulged as part of an industry training or certification process. Presumably we speak and write about what we know. When participating in computer security training and certification, such as the process involved with the preparation of this paper, participants frequently draw upon their real life and work experiences for specific examples. In the zeal to supply as much relevant information as possible, it is not uncommon to see confidential security and internal investigative information innocently shared with fellow students and conference and seminar attendees. Often no thought is given to having this information reviewed by management or legal counsel prior to disclosure and publication outside the owning company. It would be wise to sanitize and generalize any such disclosed information so as not to reveal useful specifics that might expose or advertise vulnerabilities to be potentially exploited.

Internal Threat Management

The computer risk management model can be employed to address internal threat evaluation.

Step 1, System Characterization, can be used as a means of defining the scope and boundaries of a computer system. This includes, but is not limited to, hardware, software, internal and external connectivity, support staff and system users, and the security architecture of the system. This information can be gathered utilizing existing system documentation, conducting interviews of staff supporting and managing the system, as well as use of scanning tools to identify system components.

Step 2, Threat Identification, can be focused on internal human threats. These can be mistakes caused by improperly trained employees. They can come about as a result of employees having access privileges beyond those needed or beyond the ability of the user to understand and apply. They can be caused by disgruntled or terminated employees. Human threats can arise from negligence, dishonesty or intentional maliciousness. The result of a step 2 analysis should be a threat statement, listing system vulnerabilities subject to exploitation by insiders.

Step 3, Vulnerability Identification, can identify problems existing in the system that an insider could take advantage of. Automated vulnerability and penetration testing tools can be employed to assist with this task.

Step 4, Control Analysis, consists of a review of existing controls to address the identified insider threats, and an evaluation of any threats for which additional controls are indicated.

Step 5, Likelihood Determination, focuses on assigning an indicator (low, medium, high) of the likelihood that a motivated and capable insider can exploit a known vulnerability given existing controls.

Step 6, Impact Analysis, indicates the adverse impact to the organization should a potential vulnerability be successfully exploited by an insider, e.g., unauthorized disclosure or loss of confidential or proprietary information.

Step 7, Risk Determination, speaks to the determination of the level of exposure (low, medium, high) that an insider threat to a system vulnerability will be successfully realized given the existing control environment.

Step 8, Control Recommendations, identifies recommended controls to reduce or eliminate the identified insider threats. Controls can be specific, automated solutions, such as DirectoryAlert and ServerAlert, two security products offered to network managers by NetVision, allowing insider attack attempts to be monitored. Controls can also be security processes, which encompass risk avoidance behaviors, such as watching for known network vulnerabilities and continuously monitoring network activities.

Step 9, Results Documentation, concludes the process by presentation of the identified insider threats, vulnerabilities, risks and suggested controls.

Several examples of potential insider threats appear obvious, as in the case of an employee or outside vendor who is no longer associated with the organization. This can include an employee who resigns, retires or is discharged for cause. It can also include a vendor who withdraws from providing services, losses a bid to continue providing existing services, or whose business relationship is otherwise terminated with the organization (including an employee of the vendor working with or inside the organization). Procedures must be put in place and adhered to for the immediate revocation of access to the organization's system network. (Barman)

Another threat, and possible fix, is to limit internal access and trust relationships on the system. Firewalls can be used to shield critical functions inside the organization's network by providing additional security through limited access to insiders on a need-to-know basis. This need-to-know analysis can include a review of existing employees whose access authorizations change, e.g., a job transfer to a new assignment with different system area authorizations. When new user authorizations are added, old, unneeded ones must be revoked.

Logs should be maintained and retained that will identify internal users who access system functions. The ability of insiders to erase or delete these log trails should be restricted to the degree technically possible consistent with business needs.

Another component of cybersecurity to deter insider attacks is to limit insider access to physical facilities of the network system and to restrict outside visitor access. This has become even more pressing for businesses involved in the area of health care. Following the promulgation of federal regulations regarding privacy and security under the Health Insurance Portability and Accountability Act (HIPAA), entities, dealing with patient or member medical records containing protected health information, must address administrative, physical and technical safeguard issues relating to the confidentiality, integrity and availability of such information. (Wiley Rein & Fielding, April, 2003)

Intrusion detection systems (IDS) can be used to defend against insider attacks. IDS protection is not just for external, incoming threats. It should also

be deployed inside perimeter defenses to thwart internal attacks as well. "The main issues that need to be addressed in preventing and detecting insider attacks include: what the basic problems of insider attacks are, how IDS systems can help solve the problem, and finally how an internal IDS system should be deployed using various IDS technologies." (Einwechter) IDS systems can detect, log and report attacks. They can also be used proactively to ascertain trends and patterns that might indicate suspicious network activity and violations of company use policies. Additionally, IDS logs can provide an audit trail to document improper and illegal activity that has taken place on the network and can be used for employment decision-making, defense against civil lawsuits brought by terminated employees, and for possible criminal referrals to appropriate law enforcement agencies.

IDS systems can be used in a variety of ways as a protection against insider attacks. They can be installed as network taps between routers, hubs and switches in the system. They can be specifically applied to servers. They can be used to compare normal file structure, contents and the state of activity of the network and alert when unusual modifications are made or suspicious patterns emerge. Information from multiple monitoring and detection logging sources within the IDS system can also be assembled and presented in a combined format allowing easier review and assessment for problematic patterns. Any such centralized monitoring and detection record must itself be protected from modification, destruction and unauthorized access. A well-devised and successfully implemented internal Intrusion Detection System will allow the monitored network to detect, investigate and identify insider attacks. Once alerted to any attack, the network owner can respond to prevent, stop and /or neutralize this unwanted activity.

Best practices for dealing with insider attacks, or ideally, dealing with the likelihood of insider attacks prior to actual attacks being launched, involves comprehensive planning and intertwined employment and security policies. (Scalet) Companies should carefully check and screen all internal employees they hire. Employers should also carefully check external employees they allow inside their protected areas of trust and not rely solely on the outside vendors or contractors employing the externals to perform competent and complete background checks.

Any internal or external employee or outside vendor, contractor or consultant should be provided with limited access within the computer network, having only such access as needed for assigned job functions or designated contract business purposes. Areas within the network should be protected from unauthorized access, even by users within the external barriers erected to keep intruders outside the firewalled perimeter. Computer network security should be built on the front end, and from the inside out. Network Intrusion Detection Systems can be employed as well as network activity monitoring. Security concerns and policies must be made a strong and consistent part of the company culture, users must be properly trained and adequately monitored, and any violations of these policies must be swiftly, consistently and severely dealt with.

Network and physical facilities access must be immediately terminated for any employees or associates whose business connection with the company is ended. Timely and proper coordination between the employing function, human resources, and physical security departments has to be effective in order to protect the network. Whether an employee or associate has retired, been terminated for cause, laid off, or granted a leave of absence, once that person no longer has a business need to access the network and move around inside it, all log in id's and passwords and network privileges must be revoked.

Protecting against insider threats is ultimately people driven, not technology driven. Relying on technical fixes alone may prove disappointing. Each new security product developed comes under attack and may be neutralized by hackers who make their discoveries openly available on the Internet. Optimal network protection from insider attacks revolves around active screening of employees and monitoring of system processes with reliance upon human interpretation, evaluation and intervention.

References

Allen, Steve. "Go to Jail for Downloading? Downloading MP3's Could Be Stealing". www.mp3.about.com/library/weekly/aa061200.thm

Barman, Scott. Writing Information Security Policies. New Riders Publishing, 2001. Appendix C Sample Policies.

Bickel, Bill. "And What's on Your Hard Drive". Crime/Punishment. July 30, 2001. www.crime.about.com/library/weekly/aa073001a.htm

Brenton, Chris & Hunt, Cameron. Active Defense A Comprehensive Guide to Network Security. Sybex Inc., 2001, p.6.

Carr, Jim. "Strategies & Issues: Thwarting Insider Attacks". Network Magazine, 09/05/02. www.networkmagazine.com/article/NMG20020826S0011).

Carroll, John M. Managing Risk A Computer-Aided Strategy. Butterworths Publishers, 1984, p.55.

Computer Science and Telecommunications Board. Cybersecurity Today and Tomorrow: Pay Now or Pay Later. National Academy Press, Washington, D.C., 2002, p.2.

Computer Security Institute. "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row", April 7, 2002. www.gocsi.com/press/20020407.html

Crume, Jeff. Inside Internet Security, What hackers don't want you to know … Addison-Wesley, 2000, pp. 86 & 87.

Einwechter, Nathan. "Preventing and Detecting Insider Attacks Using IDS". March 20, 2002. www.securityfocus.com/infocus/1558

Escamilla, Terry. Intrusion Detection Network Security Beyond the Firewall. John Wiley & Sons, Inc, 1998. p.182.

Fisher, Dennis. "Sites Offering Pirated Software on the Rise". October 31, 2001. www.eweek.com/article2/0,3959,128970,00.asp

Gaudin, Sharon. "Study looks to define 'insider threat'". Network World, 03/04/02. (www.nwfusion.com/news/2002/130577_03-04-2002.html).

"Insider Attacks Threat". Netvision. (www.netvision.com/security/alert.html).
Naraine, Ryan. "Pirated Software Still an Issue in High-Tech". March 20, 2003. www.internetnews.com/bus-news/article.php/2120741

Kennedy, Robert. "Using Pirated Software An Issue Many Schools Avoid". www.privateschool.about.com/library/weekly/aa030303a.htm

National Institute of Standards and Technology Special Publication 800-30. (October 2001) CODEN: NSPUE2 "Risk Management Guide For Information Technology Systems" p.1.

Scalet, Sarah D. "How to manage and prevent 'insider' attacks". CIO Security News, June 07, 2002. www.ciobriefcase.com/articles/2002/0607/insider.attacks/insider.attacks.html

Shannon, Bradley Scott. "The Jurisdictional Limits of Federal Criminal Child Pornography Law". University of Hawaii Law Review, Summer 1999. www.lpitr.state.sc.us/code/tl16c003.htm (p.23).

Swanson, Sandra. "South Carolina law requires computer technicians to report names and addresses of computer users with child pornography on their machines". July 30, 2001. www.informationweek.com/story/IWK20010730S0008.

Verton, Dan. "Analysts: Insiders may pose security threat". October 15, 2001. www.computerworld.com/securitytopics/security/story/0,10801,64774,00.html

Waggoner, Daniel, Hall, Shelley, and Wilcox, Rochelle. "Sex on the Net: Recent Cases Addressing Criminal Liability for Internet Providers". Find Law for Legal Professionals.

Wiley, Rein & Fielding. "Workplace Privacy: Steps Your Company Can Take to Reduce the Risk of Litigation". Privacy In Focus, February 2003. www.wrf.com/newsletters.asp

Wiley Rein & Fielding. "Getting a Handle on the New HIPAA Security Regulation". Privacy In Focus, April 2003.