Global Information Assurance Certification Paper

Security Auditing

Submitted April 12, 2002

Abstract:

That computer security issues are on the rise should be no great surprise. The war is on and shows no sign of slowdown. Very few days go by where we are not confronted with a new vulnerability, another exploit or some other security breach.

As network administrators install new anti-virus signatures, they know that it will be just a matter of days until another one is released needing to be installed. We patch a network vulnerability wondering what problems the fix will cause and when the next patch will be released. It is truly a never ending process, but one that can be better managed by implementing a formal security audit process that includes using both internal and external resources.

This paper describes the process of planning and conducting a security audit and the benefits of using both internal and external audit resources.

Introduction:

Let's face it; things are only going to get worse before they get better. The Computer Emergency Response Team (CERT) published the following statistics:

Year	Number of Vulnerabilities Reported	Number of Security Incidents
1999	417	10,000
2000	1,090	21,756
2001	2,437	52,658

Source: CERT/CC Statistics 1988-2001

While it is common knowledge that information security problems are on the rise, the surprising issue is the exponential increase depicted by the numbers above.

Below I've listed the highlights of the Seventh Annual Computer Crime and Security Survey conducted by the Computer Security Institute (CSI) with participation of the San Francisco FBI Computer Intrusion Squad.

Highlights of the "2002 Computer Crime and Security Survey" published by CSI on April 7, 2002 include:

- *Ninety percent (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.*
- *Eighty percent acknowledged financial losses due to computer breaches.*

- *Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.*

- *As in previous years, the most serious financial losses occurred through theft of proprietary information (41 respondents reported $170,827,000) and financial fraud (40 respondents reported $115,753,000).*

- *For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).*

- *Thirty-four percent reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)*

Respondents detected a wide range of attacks and abuses. Some examples of attacks and abuses on the rise:

- *Forty percent detected system penetration from the outside.*

- *Forty percent detected denial of service attacks.*

- *Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).*

- *Eighty-five percent detected computer viruses.*

- *Thirty-eight percent suffered unauthorized access or misuse on their Web sites within the last twelve months. Twenty-one percent said that they didn't know if there had been unauthorized access or misuse.*

- *Twenty-five percent of those acknowledging attacks reported from two to five incidents. Thirty-nine percent reported ten or more incidents.*

- *Seventy percent of those attacked reported vandalism (only 64% in 2000).*

- *Fifty-five percent reported denial of service (only 60% in 2000).*

- *Twelve percent reported theft of transaction information.*

- *Six percent reported financial fraud (only 3% in 2000).*

The above highlights were taken directly from CSI's press release dated April 7, 2002 and can be found at the following URL: http://www.gocsi.com/press/20020407.html

Patrice Rapalus, CSI Director, remarks that the "Computer Crime and Security Survey," has served as a reality check for industry and government:

> "Over its seven-year life span, the survey has told a compelling story. It has underscored some of the verities of the information security profession, for example that technology alone cannot thwart cyber attacks and that there is a need for greater cooperation between the private sector and the government. It has also challenged some of the profession's 'conventional wisdom,' for example that the 'threat from inside the organization is far greater than the threat from outside the organization' and that 'most hack attacks are perpetrated by juveniles on joy-rides in cyberspace.' Over the seven-year life span of the survey, a sense of the 'facts on the ground' has emerged. There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace. Post-9/11, there seems to be a greater appreciation for how much information security means not only to each individual enterprise but also to the economy itself and to society as a whole. Hopefully, this greater appreciation will translate into increased staffing levels, more investment in training and enhanced organizational clout for those responsible for information security." (http://www.gocsi.com/press/20020407.html)

The numbers and responses above clearly present the reality of security management today. Knowing the current status of your company's security methods is the first step in proactive security management and a full security audit is the best way to achieve this goal. (*The Info-Tech Research Group Security Auditing: An Eight Step Guide, , 2001)*

A security audit is a systematic assessment of policies and procedures that have been implemented to safeguard information assets. You can choose to focus the audit on different areas (as we will see in the Risk Assessment Section), however, a security audit "will address issues with IT systems, including hardware and software, infrastructure (such as cabling, telecom), procedures and business processes and people" *(Justin Kapp, How to Conduct a Security Audit; PC Network Advisor Article T04123.1)*

It is important to understand the difference between a security audit and the more traditional EDP audit (also know as application audits) which is typically conducted during a financial audit. The EDP audit involves reviewing company standards for development, change management, application security and process management. As we will see, a security audit is more concerned with the degree of compliance with company security policies.

Security auditors are typically divided into two categories, internal and external. The internal auditor is usually employed by the organization and performs auditing in addition to other network administrative duties. Traditionally, external security auditors have been Certified Public Accountants (CPA) or other audit professionals hired to perform independent financial audits. Today, many security professionals have come from a technical background and are performing independent security audits. The topic of audit independence is covered in a later section.

The purpose of this paper is to present the primary steps involved in preparing for and actually conducting a **security audit** with emphasis on employing a cooperative methodology for using both internal and external resources. This paper includes the following sections:

1. The starting point: Risk Analysis and Assessment
2. The security policy
3. The five-step audit plan
4. Benefits of internal and external audit resources
5. Conclusion

Section 1: Risk Analysis and Assessment

All organizations, whether formally or informally, conduct a risk assessment when they decide which IT assets to secure (and to what level). For example, deploying biometric security to restrict access to the server room might be considered prudent given the potential damage that could result from unauthorized access. However, in most cases, deploying similar controls at the workstation level would be considered "overkill" and could not be cost justified.

It is important that the person (or group) performing the audit have a sense of the relative worth of IT assets to the company. The following steps will help you conduct a risk analysis and aid in defining the level of scrutiny to apply to each IT asset during the audit:

- Inventory all IT assets and develop network topology maps. Hopefully, both of these are readily available.
- Conduct interviews with key users and data owners to determine the relative worth of their data. Always expect users to inflate the value of their given process / data – but be mindful to correlate dependencies from other areas of the business.
- Assess the impact to the organization of losing key systems and data sets. The impact of losses can always be measured, either directly or indirectly, in dollars. For example, downtime on e-commerce sites results in abandoned shopping carts reducing sales and e-mail disruptions caused by virus attacks results in lost employee productivity increasing payroll expenses. This quantitative amount can be used to assess the cost justification for enhanced security measures.
- Lastly, have discussions with company executives and decision makers. IT assets that support these groups should be appropriately safeguarded.

Risk is a combination of the probability of some event occurring combined with the size of the impact on the organization. These risk factors, if properly measured, can aid in defining the scope and breathe of the security audit.

Section 2: The Security Policy

Before you begin a security audit, it is a good idea to review and understand the company's security policies. The security policy, used with the above risk analysis, will serve to properly focus the audit on those assets considered a "higher" risk.

It is important to realize the many companies do not have formally documented security polices and tend to rely on informal, traditional rules that have been implemented overtime. Understanding and documenting these rules will enable the auditor to better focus on those audit subjects that are critical to the organization's operation.

The absence of a formal security policy is, in itself, a significant issue which would need to be addressed with the organization's management during the course of the audit. The security policy is the foundation of the company's information security.

Section 3: The Five-Step Audit Plan

Step 1: Preparation and Management Buy-in

Proper planning is critical in order to improve the odds of a successful security audit. This is true whether the audits are conducted by internal or external resources, or both. The following steps need to be performed to adequately prepare for conducting a comprehensive security audit:

- Clearly identify the audit objectives based on:
  - Risk assessment and analysis
  - Management concerns
  - Industry best practices

- Identify and obtain the needed tools and resources for completing the audit (including access to hardware, software and people). This includes issues of coordinating the timing of tests (for example, you should not plan to audit the accounting server during the month-end close).

- Implement comprehensive project planning to organize and monitor the audit process. Included are distributing periodic status reports and meeting with management on the progress of the audit. The frequency of these meetings is dependent on management availability and the length of the audit. The bottom line is that the auditor needs to communicate effectively and timely with management to avoid surprises.

- Communicate the audit objectives, timing and deliverables to the organization's decision makers to manage expectations. In addition, it is strongly recommended to obtain written permission to perform audit procedures from the appropriate management level.

An integral part of preparing for an audit is to manage the expectations of the user community. An audit stands a much greater chance of being successful if management buy in is communicated to all levels within the organization.

Step 2: Information Gathering

Gathering information is actually divided into two main categories:

1. People information, and
2. System testing

People Information –

The audit process needs to include conducting both formal and informal interviews with IT staff, end-users, managers and anyone who has access to the site. This is an often overlooked step, but a critical one. A recent FBI study found that 81% of the respondents indicated that the most likely source of a security breach is from inside the company. Interviews with the user community will enable the auditor to assess the general compliance with corporate security policies and uncover potentially dangerous situations and/or policies. We have all heard of the system administrator who religiously performs daily server backups only to find out that the CFO is storing files locally (and are not being backed-up). Of course, this situation is typically uncovered when the CFO requests a file he just accidentally deleted for an upcoming meeting with the Board of Directors.

Systems Review & Testing -

Gathering technical information should be accomplished with various static audit tools. These tools are available as both freeware (some shareware) and from commercial independent software vendors (ISV). While it is considered a "best practice" to use multiple tools, factors including cost, duration of audit, timing and reporting requirements will influence whether free scanning and vulnerability tools are selected or various commercial software is used during the audit. Regardless of the tools employed, the auditor must be sufficiently trained to use them before the start of the audit process. If not, it will become apparent and the audit results will be suspect.

Listed in Exhibit 1 are various tools by functional category. Of course, some of these tools perform multiple functions. This list is far from complete, but should serve as a good starting point for finding tools to automate various audit functions.

Below I have outlined some of the major audit areas that should be addressed during the system review and testing:

- Review highly privileged user accounts.

- Scan for non-essential services.
- Verify user password policy is enforced and examine password effectiveness.
- Look for unauthorized software and hardware on the network.
- Review all system and application logs, including operating system, firewall, IDS and other security related systems.
- Check physical security accommodations.
- Review all access change control procedures (as established by policies and procedures).
- Examine setup of security defenses for improper or incomplete configurations. Remember that most vulnerabilities result from improper setup, installation or maintenance and not program bugs.
- Examine the level of operating system and application hot fixes and security updates.
- Analyze the effectiveness of "defense in depth" as deployed by the company within the boundaries of the audit objectives.
- Analyze the IT groups' use of security related log files. If no-one is reviewing the firewall logs, how can we measure its effectiveness?
- Perform a comparative analysis of the current audit results with a pervious baseline (if available).

An important rule during this phase, as pointed out numerous times during the SANS GSEC, is to confirm any significant finding through alternate means. This could be the use of alternate tools or simply reviewing a "draft" of the final audit report with the IT group. What may appear as a security breach might just be the night janitor playing MS Solitaire.

Step 4: Data Review and Report Write-up

During the information gathering phase, the auditor will accumulate an enormous amount of raw data and observations. Making use of effective tools to automate the analysis of the data collected can expedite the reporting process.

The auditor needs to meet with the appropriate people to discuss the preliminary findings as a part of preparing the final report. At this time, discussions can cover future action items to address issues that have surfaced as a part of the audit. The major sections to include in the report should be:

1. An executive summary reflecting the audit objectives and the major issues uncovered.
2. A review of the audit plan outlining what was and what was not tested (any why).
3. A detailed comparative analysis between the current audit and a previous baseline (if available).

4. A statement of overall compliance with established policy.
5. A prioritized listing of action items with a cost / benefit analysis for each item.

It is critical that the presentation of the reports reflect the technical level of the intended audience. As the target audience is typically upper management, the report needs to be clear and concise, computer jargon-free and speak to the business issues of securing IT assets.

Step 5: Post Audit and Administrative Issues

Typically, management will not authorize all the recommendations that are suggested by either internal or external auditors. While the suggestion makes perfect sense to the "technical" staff, and it is cost justified, there are times when the risk factor is acceptable to the decision makers (who, incidentally, will not be present during the all-nighter needed to rebuild that server).

As such, it will more than likely be necessary to redraft the action items to accommodate the management's directives. Of course, it is a good idea to keep a record of all recommendations and simply update those not currently approved by management and why.

Spending sometime on post audit administrative issues can serve to expedite future audits. The following steps are recommended:

- Make a secure copy of all data accumulated during the audit and store off-site. This can serve as a comparative baseline for future reviews.
- Analyze the effectiveness of the audit plan and document changes for future reviews.
- Analyze the suitability of tools used during the process documenting problematic issues.
- Document the major challenges encountered during the audit and take steps to mitigate them during future audits.

Section 4: Benefits of internal and external resources

During the course of this paper, we have made very little distinction between the use of internal and external auditors. The fact of the matter is that the best scenario is where both groups are used to improve each others effectiveness (from the eyes of the organization). For the organization, improving the effectiveness of the external resources is measured by improved services at a lower cost. This can

be achieved by improving the technical competence of internal resources by participation in the audit process.

An independent audit is not intended to replace the internal audit function, but rather compliment their activities.

In a recent article posted at Searchsecurity.com, Neil Jackson (business manager, internal audits, E*Trade Financial) was quoted:

"Preparing for an audit starts with a company understanding the need for an audit and accepting its added value to their organization and business objectives. Some companies look at audits as necessary evils. However, planning for an audit requires (the company) accepting why auditing is good for the business and expecting to take the audit's findings as positive criticism and moving forward." Edward Hurley, "Auditor: There's nothing to fear". URL: http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci815576,00.html

The point being made is that audits need to be view as a positive engagement where internal resources can learn from external ones. This will enable the external auditors to leverage off the internal auditor's work resulting in a more secure environment, at a substantially lower cost. Companies do benefit from bringing in outside expertise. These advantages include using the most recent methodologies to technical knowledge transfers to inside employees.

The last issue to address in this section is the concept of auditor's independence. As with CPA's, it is critical that Information Systems Auditor "…be independent of the auditee in attitude and appearance" *(IS Auditing Guideline, Document #020.010.010, ISACA).* This concept applies equally to internal and external auditors. Of course, special checks and balances may need to be established as it relates to internal auditors. For example, the internal security auditor may need to report to the CEO rather than the CIO to maintain a level of independence.

The recent financial scandal at Enron is a perfect example, although quite extreme, of what can happen when independence is violated. While this related to a financial audit, lessons can be learned and applied to security audits. Although it is not a current requirement, as systems become more and more connected and companies are increasingly dependent on those systems, we are going to see increased requirements for formal security audits from the financial and investor communities (similar to current financial audits).

Section 5: Conclusion

Performing both internal and external security audits is critical to the success of any business that uses computers. A security audit is no longer a once-a-year project conducted by an outside group. Security management is an on-going process that is best managed using both internal and external resources.

The organization that relies on a security vendor's promise of integrity is being foolish at best. When something goes wrong, it's not the vendor's business on the line (at least not immediately).

While no two audits are the same, the steps outlined in this paper will enable you to insure that your organization is systemically managing security issues and using effective, proven techniques.

Exhibit 1

Example Auditing Tools

Name	Web Link
Port Scanners	
Nmap	www.insecure.org/nmap/
NTmap	www.eeye.com/html/Research/Tools/nmapnt.html
SuperScan 3.0	www.foundstone.com
LANguard 2.0	www.gti.com
Password Crackers	
@stake lc3	www.atstake.com
John the Ripper	www.openwall.com/john
Lostpasswords.com	www.lostpasswords.com
Vulnerability Scanners	
BindView	www.bindview.com
Nessus	www.nessus.org
Stat Scanner Professional	www.statonline.com
NetIQ Security Analyzer	www.webtrends.com
Realsecure	www.iss.com
MS Baseline Security Analyzer	www.microsoft.com/security
CSI W2K Level I Benchmark	www.cisecurity.org
Security Space (Internet based scanner)	www.securityspace.com
Packet Sniffers	
Tcpdump	www.tcpdump.org
CommView	www.tamos.com
Ethereal	www.ethereal.com

All links active at 4/10/2002

References:

1. Justin Kapp, "How to Conduct a Security Audit". URL: http://itp-journals.master.com/texis/master/search/?q=T04123.1&s=SS
2. C&A Security Risk Analysis Group, URL: http://www.security-risk-analysis.com
3. Ed Orton and Nahum Goldmann, "The Critical Role of Independent Security Audits". Version 08/04/2002: ADDSecure.Net Inc.
4. Information Systems Audit and Control Association, "IS Auditing Guideline – Effect of Nonaudit Role on the Auditor's Independence", Document #020.010.010. URL: www.isaca.org
5. Computer Security Institute, "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row". URL: http://www.gocsi.com/press/20020407.htm
6. D. Ian Hopper, "Computer Hacking Up, FBI Finds". URL: http://enterprisesecurity.symantec.com/content.cfm?articleID=1267&PID=11390356&EID=186
7. Michael S. Mimoso, "Security audits a burden, blessing to CEOs". URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci811614,00.html
8. Edward Hurley, "Auditor: There's nothing to fear". URL: http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci815576,00.html
9. Info-tech research group, "Security Auditing: An Eight-Step Guide". 2001
10. Ronald L. Krutz and Russell Dean Vines, The CISSP Prep Guide. 2001
11. Harold F. Tipton and Micki Krause, Information Security Management Handbook – 4th Edition. 2000
12. CERT/CC Statistics 1988-2002, URL: http://www.cert.org/stats/cert-stats.html#incidents

All links active at 4/10/2002