Intrusion Detection and Information Security Audits

Terry T. Kidd
University of Texas Health Science Center, USA

Robert K. Hiltbrand
University of Houston, USA

INTRODUCTION

The rapid expansion and dramatic advances in information technology in recent years have without question generated tremendous benefits to business and organizations. At the same time, this expansion has created significant, unprecedented risks to organization operations. Computer security has, in turn, become much more important as organizations utilize information systems and security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Such use of computer security is essential in minimizing the risk of malicious attacks from individuals and groups. To be effective in ensuring accountability, management and information technology security personnel must be able to evaluate information systems security and offer recommendations for reducing security risks to an acceptable level. To do so, they must possess the appropriate resources, skills, and knowledge.

With the growing perverseness of information systems and the technologies used to support such tools, the growing need to keep the integrity of both the data and the system used to manage that data will become a major priority. Therefore, it is important for security personnel and management to keep abreast of the issues and trends in information systems and security, and the tools and techniques used to secure systems and data.

In order to keep information safe and systems secured from outside attacks from computer criminals, information systems security and network vulnerability assessment must be conducted on a regular and ongoing basis to insure system security integrity. The aim of this article is to introduce to the information technology community, the conceptual overview of information security audits. Not only will this article present an overview of information security audits, but also information on popular intrusion detection and security auditing software used in industry.

BACKGROUND

Advances in information systems and the technology used to support those systems have produced great results for organizations, businesses, and other agencies in terms of work productivity, information storage, management, and in opportunities for the competitive advantage. While the promise and offerings of information systems have tremendous benefits, information systems have also created significant and unprecedented levels of risks to organizational operations. Businesses, hospitals, schools, universities, governmental agencies, and banks depend heavily on information systems, thus increasing the need for information security. With this newfound dilemma, organizations are beginning to use information security measures to ensure that the integrity of other data is held at an optimal level.

As discussed previously, the aim of information security used by an organization is to avoid data tampering, fraud, inappropriate access to and disclosure of sensitive information, and disruptions in critical operations (Umar, 2003). Unfortunately, these risks are expected to escalate as wireless communication technologies emerge and become ubiquitous. If information systems personnel are to be effective instruments of accountability and assessment, they need to be able to evaluate information systems and security measures to offer recommendations for reducing the security risk to an acceptably low level (Umar, 2003).

Further, the growing importance of information systems in performing daily operational activities, along with the elimination of paper-based evidence and audit trails, demands that these professionals consider the effectiveness of information technology security controls during the course of financial and performance audits. To do so, information security personnel must acquire and maintain appropriate resources and skill sets to help prevent computing security threats, vulnerabilities, or attacks. This can be a daunting challenge in an era of rapid evolution and deployment of new information technology. Likewise, management within organizations needs to take stock of their information systems security audit and its capabilities, to ensure that strategies exist for their continued development and enhancement, for an organization's security is only as strong as its policy.

When it comes to articulating or writing the organization security policy, the discussion should be more than information systems and the technologies used to support those systems, the conversation should move past a discussion of infrastructure (e.g., hardware and software), but to a discussion of security and methods for securing the organization's systems and most valuable assets—its information.

According to Holden (2004), information is essential to the achievement of any business or organizational. Its reliability, integrity, and availability are significant concerns in most organizations. The use of computing and system networks, particularly the Internet, is revolutionizing the way organizations conduct their business and their day-to-day operations. While the benefits of such tools have been enormous and have allowed vast amounts of information to be available at our fingertips, these interconnections also pose significant risks to computer systems, information, and to the critical operations and infrastructures they support. Infrastructure elements such as telecommunications, power distribution, financial data, research and development information, as well as personnel data are subject to these risks. The same factors that benefit operations—speed and accessibility—if not properly controlled, can leave them vulnerable to fraud, sabotage, and malicious or mischievous acts (NSAA & GAO, 2001). In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected. Recent publicized disruptions caused by virus, worm, and denial of service attacks on both commercial and education Web sites illustrate the potential for damage.

Information security is of increasing importance to all levels of organization management in minimizing the risk of malicious attacks from individuals and groups. These risks include the fraudulent loss or misuse of organization resources, unauthorized access to release of sensitive information such as tax and medical records, disruption of critical operations through viruses or hacker attacks, and modification or destruction of data. According to the National State Auditing Association and the General Accounting Office (NSS & GAO, 2001), the risk that information attacks will threaten vital organization interests increases with the following developments in information technology:

- Monies are increasingly transferred electronically between and among governmental agencies, commercial enterprises, businesses, and individuals.
- Organizations and businesses are rapidly expanding their use of electronic commerce.
- Business, government, and national/domestic security communities increasingly rely on the available information technology.
- Public utilities and telecommunications increasingly rely on computer systems to manage everyday operations.
- More and more sensitive economic and commercial information is exchanged electronically.
- Computer systems are rapidly increasing in complexity and interconnectivity.
- Easy-to-use hacker tools are readily available, and hacker activity is increasing.
- Paper supporting documents are being reduced or eliminated.
- Each of these factors significantly increases the need for ensuring the privacy, security, and availability of state and local government, business, and public education systems.

Although as many as 80% of security breaches are probably never reported, the number of reported incidents are growing dramatically with relative intensity (NSAA & GAO, 2001). To further illustrate the need for information systems security, a survey conducted by the Computer Security Institute in cooperation with the FBI found that 70% of respondents from large corporations and government agencies had detected serious computer security breaches within the last 12 months and that quantifiable financial losses had increased over past years (NSAA & GAO, 2001).

Are organizations responding to the call for greater security? There is great cause for concern regarding this question, since earlier reports of analyses on computer security identified significant weaknesses. The weaknesses identified place a broad array of organizational and business operations as well as assets at risk of fraud, misuse, and disruption. Further, information security weaknesses can place enormous amounts of confidential data, ranging from personal, financial, tax, and health data to proprietary business information, at risk of inappropriate disclosure. According to the National State Auditing Association and the General Accounting Office (NSS & GAO, 2001), typical information technology computer security weaknesses in an organization include the following:

- lack of formal planning mechanisms with the result that they do not serve the organization's pressing needs or do not do so in a timely and secure manner
- lack of formal security policies resulting in a piecemeal or "after-an-incident" approach to security
- inadequate program change control, leaving software vulnerable to unauthorized changes
- little or no awareness of key security issues and inadequate technical staff to address the issues;
- failure to take full advantage of all security software features such as selective monitoring capabilities, enforcement of stringent password rules, and review of key security reports
- inadequate user involvement in testing and sign-off for new applications resulting in systems that fail to meet user functional requirements or confidentiality, integrity, and availability needs
- installation of software or upgrades without adequate attention to the default configurations or default passwords
- virus definitions that are not kept up to date
- inadequate continuity of operation plans
- failure to formally assign security administration responsibilities to staff who are technically competent, independent, and report to senior management

Also of concern is a relatively recent threat—weaknesses in operating systems. A number of business and organization Web sites were hacked through a vulnerability in a widely used operating system. The time between the discovery of the vulnerability by the vendor and the notification to users that a special software patch should be applied was a matter of days and sometimes weeks (NSAA & GAO, 2001). The need for immediate notification of vulnerabilities and a subsequent need to react immediately will mean higher standards for security and network system administration groups who may have limited staff and technical knowledge. This is why the need for information systems security auditing is important and thus valuable to the integrity of an organization.

Systems Security Audits

With the growing need for security measures and the limited number of technical staff to meet the demands for the ever-increasing threat of unauthorized intrusion into an organization's networking system, security audits have become one of several lines of defense employed to help mitigate such action. According to Haynes (2003), a security audit is a process that can verify that certain standards have been met and identify areas in need of remediation or improvement. Dark and Poftak (2004) add that a computer security audit involves a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site or location. Current literature suggests that computer security auditors work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited. In times past, identifying problem areas in a system had to be done by a team of human auditors, but now software can analyze a computer, a system, or a range of systems, and present the evidence that you do not need to be an expert to comprehend. It is important to use software that stays current with the rapidly evolving security threats. Software cannot resolve the entire problem of intrusion, but it helps in the process. Computer users within organizations need to assess, evaluate, discuss, run reports, make changes to corrections to the problems, and then rerun the reports in order to ensure maximum integrity and optimization of a network system. When success is achieved in resolving all the identified problems, we can raise the bar on the standards we are trying to achieve.

Haynes (2003) further explains that a security audit is a policy-based assessment of the procedures and practices of a site, assessing the level of risk created by these actions. A security audit comprises a number of stages. You can choose to focus the audit on different areas, such as the firewall, host, or network. However, a security audit will address issues with your systems, including software and hardware, your infrastructure, your procedures, your business processes, and your people. Information is the key. Once the audit has been completed you will have information on the compliance level of the users and systems under your control, with an idea of the risk exposure and security level of these systems (Haynes, 2003; Dark & Poftak, 2004). You will also have an idea of the potential damage that could occur if the worst came to the worst—this enables you to plan and develop a strategy to ensure minimal damage. In some cases management may choose to carry out an audit internally or use an external contractor. Whoever carries out the audit, those personnel should have the relevant technical expertise and ability to communicate the findings of the audit. It is also important that the auditor has an understanding of the organization under review. When auditing an information system that holds data that requires security clearance from upper management, the auditor must have the required clearances in order to access the systems holding that specified data (Haynes, 2003; Dark & Poftak, 2004).

According to Lerida, Grackzy, Vina, and Andujar (1999) when one conducts a security audit it is important to look beyond the systems and consider the human interface to those systems. This is on the same lines as Kapp (2000), Haynes (2003), Dark and Poftak (2004), and Stair and Reynolds (2006). One may think their system is perfectly secure, but the users may be involved in practices that compromise the security of the systems in place. This may include surfing unauthorized Web sites, installing shareware and peer-to-peer applications or transferring virus-infected e-mails and desktop applications. As a result any audit must attempt to identify all the possible risks. Information systems and the technologies used to support those systems are at risk from compromise from a number of sources, including poorly managed or badly configured systems, internal users, external users, and external attackers (sometimes known as crackers or hackers). It is important to understand that these attacks can come from a variety of sources and thus have to be analyzed in depth. A point to remember is that security audits do not take place in a vacuum; they are part of the ongoing process of defining and maintaining effective security policies (Kapp, 2000). It involves everyone who uses any computer resources throughout the organization. Security audits provide a fair and measurable way to examine how secure a system or site really is. Even authorized system users can be the source of a security breach, therefore identifying possible lapses that could allow this is just as important as preventing external attack. It is important to understand that information security or computer security audits must move beyond information technology audits, which are concerned with ideas of auditing what is on the computer system and how it is being used. Instead security audits must also move past the review of programs and hardware, to the level of verifying that programs are operation with full integrity as they are intended to operate (Kapp, 2000). Security audits also must encompass components that ensure the data and information are reliable, as well as to verify that the information has not been compromised. To be successful at analyzing the security and integrity of an organization's network infrastructure, a team approach can be used to optimize security research. Security audits can be part of an information technology audit conducted by a team of professionals with expertise not only in the theoretical underpinnings of information systems, but also in the computer or networking system being audited. In addition, security audits must go beyond the annual financial audits and physical inventory audits to the data and content, which are standard processes in most businesses. Security audits look into how the data or information is stored and whether that data is secure. This is the importance of using a security auditing tool.

Methods for Performing Security Audits

When performing a security audit, one must perform the audit though personal interviews, vulnerability scans, examination of operating system settings, analyses of network shares, and historical data (Kapp, 2000; Hayes, 2003). Those who conduct the audit should be concerned primarily with how security policies—the foundation of any effective organizational security strategy—are actually applied and implemented. According to Haynes (2003), there are a number of key questions that security audits should attempt to answer concerning the audit:

- Are passwords difficult to crack?
- Are there access control lists (ACLs) in place on network devices to control who has access to shared data?

- Are there audit logs to record who accesses data?
- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up to date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?
- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

These are just a few of the kind of questions that can and should be assessed in a security audit. In answering these questions honestly and rigorously, an organization can realistically assess how secure its vital information and systems are.

Conducting a Security Audit with GFI LANguard

Over the past few years, a number of intrusion detection and vulnerability assessment tools have been developed to aid the information systems professionals in their efforts in keeping their systems secure and their data safe. These tools run on a number of platforms including Windows NT, 2000, XP, and Linux. There are a number of types of tools that detect changes in system configuration, tools that test for known security issues, and a class of tools that are used to monitor systems in real time, such as network sniffers. Of the programs available to the public on the market, one program has consistently gained favor with security professionals in the field. This particular program can be used in conjunction with other tools as one line of defense for an organization. GFI LANguard Network Security Scanner (N.S.S.) is a premier security auditing tool that checks the network for all potential methods that an unauthorized user may employ to attack or gain entry into a system. By analyzing the operating system and the applications running on the network, GFI LANguard N.S.S. identifies possible security holes. During a security audit, GFI LANguard N.S.S. scans the entire network, IP address by IP address, and alerts the auditor of the weaknesses discovered on the specified network(s). Using a combination of operating system functions together with the features offered by GFI LANguard N.S.S., one can proactively deal with the security issues detected. For example, security issues can be proactively detected by shutting down unnecessary ports, closing shares, as well as installing service packs and hotfixes before malicious persons can exploit them. By default, GFI LANguard N.S.S. allows the auditor to perform security audits on both Windows- and Linux-based target computers. During an audit, the scanning engine collects various hardware and software information from the scanned targets. This includes the service pack level of each target computer, potentially vulnerable devices such as wireless access points and USB devices, installed applications, as well as open shares and open ports (GFI Software, 2005). The scanner also enumerates specific OS configuration settings such as Windows registry settings and password policy configuration details aiding in the identification of common security issues related to an improperly configured operating system such as an OS running on default settings (GFI Software, 2005).

With this software scan, results can easily be analyzed using filters and reports, enabling the security team to proactively secure the network by shutting down unnecessary ports, closing shares, installing service packs and hot fixes, to name a few. In addition to the features listed above, GFI LANguard N.S.S. is also complete with a patch management solution system aimed at enhancing the security audits that are identified (GFI Software, 2005). After the software has scanned the network for security weaknesses and determined missing patches and service packs—both in the operating system and in the applications—one could use GFI LANguard N.S.S. to deploy service packs and patches network-wide with the ease. Not only is the software able to deploy service pack and patches network-wide, the software can also deploy custom software and updates network-wide to ensure a wider range of network security and information integrity. According to GFI Software (2005), when determining whether to use a network security scanning product on the market, one should look at the following product attributes:

- network security vulnerabilities (Windows and Linux) scanning
- intrusion detection of unnecessary shares, open ports, and unused user accounts on workstations
- network analysis for and deployment of missing security patches and service packs in OS and Office
- wireless node/link detection and USB device scanning
- ease of use and report generation

In addition to the regular use of an active network vulnerabilities scanner such as GFI LANguard's Network Security Scanner, the use of real-time (actually, near-real-time) network-based intrusion detection/prevention systems (known by the initials IDS/IPS) such as the GFI LANguard Security Event Log Monitor (S.E.L.M.) in conjunction with host-based IDS/IPS systems such as GFI LANguard's System Integrity Monitor (S.I.M.) provide defense-in-depth against both internal and external threats.

GFI LANguard's System Integrity Monitor is a utility that provides intrusion detection by checking whether files have been changed, added, or deleted on a host system. If a change happens, S.I.M. alerts the central monitoring system (e.g., GFI LANguard's Security Event Log Monitor) as well as the systems administrator or other designated personnel via e-mail and centralized event log. Since hackers need to change certain system files to gain access, this utility provides a means to further secure any host systems open to attack.

The use of both passive (intrusion detection systems) and active (vulnerability scanner) measures that are network based and host based provide the beginnings of a solid defense-in-depth strategy for securing an organization's information systems. Security is a process, not a single piece of technology, not a black box that sits in the corner, and there are no "silver bullets" that will cure all woes. Information Assurance and Computer Security are concepts, not end points. Security is a journey and not a destination. Assessment, implementation, and evaluation are the step all organizations must undertake on a continuing basis to constantly improve security and stay even with the hackers that want into your network and want unauthorized access to your precious data. Using intrusion detection software and network security auditing tools as one line of defense to any organization can be one step closer in ensuring that the organization's data contains full integrity.

CONCLUSION AND FUTURE TRENDS

In building information systems security audit procedures and policies, management should assess the organization's security audit readiness by taking into account the following relevant factors. Establishing a baseline in these areas by identifying strengths and weaknesses will help an organization determine the best way to proceed. In many instances, this process will determine what is practical to implement within given time and budget constraints. Although an organization may have time, staffing, technology, and budgeting constraints, software such as GFI LANguard presents itself to be a positive mid-range solution for those looking to optimize their network and systems security within their respective organizations. Along with experienced personnel to perform security audits, an information systems security audit capability must have the relevant tools, techniques, and practice aids available to assist the auditors with their audit tasks. Decisions on obtaining such tools, techniques, and practice aids, along with the appropriate expertise to use them, must be based on the hardware, system software, and applications that constitute the audit environment, as well as on the information security policy within the organization.

With networking systems becoming more and more interconnected, the hardware and software that make up and connect these systems are critical. The technical components that provide network, Internet, and intranet connectivity must be identified, analyzed, and reviewed on a continuous basis, in order to ensure maximum operating optimization as well as for data and information integrity (Umar, 2003). Organizations should develop an inventory of this infrastructure, which should be periodically refreshed since computer systems are extremely fluid, and projections are that technology will continue to advance rapidly. It is important to understand that information systems security is of increasing importance to all levels of organization management in minimizing the risk of malicious attacks from individuals and groups. In order to preserve the vitality of a business or an organization, information must be kept in full integrity; not doing so will ensure risks that may become detrimental to the organization, its resources, and personnel. In order to keep information safe and systems secured from outside attacks from hackers and other computer criminals, information systems security and network vulnerability assessment must be conducted on a regular and ongoing basis to insure system security integrity.

REFERENCES

Dark, M., & Poftak, A. (2004). How to perform a security audit. *Technology & Learning, 24*(7), 20-22.

GFI Software. (2005). *GFI LANguard Network Security Scanner (N.S.S.).* Retrieved May 1, 2005, from http://www.gfi.com/lannetscan

Haynes, B. (2003). *Conducting a security audit: An introductory overview. Security focus*. Retrieved May 1, 2005, from http://www.securityfocus.com/infocus/1697

Holden, G. (2003). *Guide to network defense and countermeasures.* Boston: Thompson Course Technology.

Kapp, J. (2000). How to conduct a security audit. *PC Network Advisor, 120*(7), 3-8.

Lerida, J.L., Grackzy, S.M., Vina, A., & Andujar, J.M. (1999, October 5-7). Detecting security vulnerabilities in remote TCP/IP networks: An approach using security scanners. *Proceedings of the International Carnahan Conference on Security Technology*, Madrid, Spain.

NSS & GAO (National State Auditors Association and the U.S. General Accounting Office). (2001). *Management planning guide for information systems security auditing.* Washington, DC: NSS & GAO.

Stair, R., & Reynolds, G. (2006). *Fundamentals of information systems* (3rd ed.). Boston: Thompson Course Technology.

Umar, A. (2003). *Information security and auditing in the digital age—a managerial and practical perspective.* NGE Solutions.

KEY TERMS

Information Systems: A set of interrelated components that collect, manipulate, and disseminate data and information, and provide a feedback mechanism to meet an objective.

Information Systems Security: The protection of information systems against unauthorized access (or the denial of service to authorized users) and modification of information (whether in storage, processing, or in transit), including those measures necessary to detect, document, and counter such threats.

Intrusion Detection: Software that monitors systems and network resources, and notifies network security personnel when it sees a possible instruction.

Network Security Scanner: A software program that identifies possible security weaknesses and threats.

Security Auditing: A process that can verify that certain standards have been met and identify areas in need of remediation or improvement. A security audit involves a systematic, measurable technical assessment of how an organization's security policy is employed at a specific site or location. Current literature suggests that computer security auditors work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited.

Security Policy: A policy that outlines rules for computer and information systems access. The policy determines how policies are enforced and lays out architecture of the company information security environment.

Vulnerability Assessment: The process of identifying technical vulnerabilities in computers and networks, as well as weaknesses in policies and practices relating to the operation of these systems.