Approach to Auditing Network Security

By S. Anantha Sayana

Today we live in a connected world. Communication is a key requirement for all systems. Increased integration of systems requires a compulsive need to establish fast and reliable communication that is as widespread as the organization and its business dealings. Information systems need to reach out to users, vendors, customers and partners (irrespective of their location); everything is connected to nearly everything else.

All this brings us to the issue that looking at any system as something that is inside one box or in one enclosed space is not enough to gain assurance about its security. The reality is that nearly every computer in the world could be, and in most cases is, connected to every other computer through the Internet. The worldwide propagation of the (in)famous Nimda, Code Red and Lovebug viruses and worms are proof of this connectivity. Such connectivity has the propensity to provide access or communication paths for anyone to any system in the absence of any measures to prevent such access. Fortunately, a plethora of technical solutions, many of which have become standards, keeps most networks and systems segregated and protected.

Therefore, let us look at how we fashion an approach to auditing networks and ensuring that they are secure.

It is also good to emphasize at this stage that in the overall information systems audit framework, the audit of networks is one piece of the puzzle, with the other notable pieces being audit of application software, audit of operating systems and databases, audit of physical and environmental security and audit of business continuity (these have been dealt with in earlier issues of the IT Audit Basics column). To obtain a comprehensive assurance about systems, it is important to assess and evaluate all the parts. In this issue, we will focus on auditing network security.

A network could be as simple as a small local area network (LAN) connecting a few computers inside a single room or a building, or it could be something that connects computers at factories and offices spread over a number of cities or even countries. A network could also be connected to other networks, such as the networks of customers or vendors or a public network like the Internet.

Network Vulnerabilities

The basic vulnerabilities associated with a network can be grouped into three broad categories:

1. Interception—The data that are transmitted over the network pass through some medium that consists of a carrier and other equipment, often in the physical control of other third parties. These data could be intercepted. Once intercepted, there is a risk of undesirable disclosure, i.e., someone stealing data or modifying the intercepted data, resulting in loss of integrity and consequent other, more material losses.
2. Availability—As networks proliferate, more and more users are remote and access their applications over the network, crossing hundreds or thousands of miles. If network connectivity fails or becomes unavailable for any reason, there would be serious interruption to business and consequent damages.
3. Access/entry points—The network extends a computer system beyond the box into the world. The network provides the ability to extend the system to users across geographical boundaries, resulting in conveniences and efficiencies otherwise impossible. Conversely, the same network provides the feasibility for access to the system from anywhere. A single weak point in the network can make all the information assets in the network vulnerable to intruders. The network can provide many points of entry for intruders, interceptors and malicious code-like viruses, worms and Trojan horses. The ability of the network to enable access to a system from anywhere is the most serious of a network's vulnerabilities. Given the fact that a major benefit of a network is its ability to provide access from elsewhere, the task at hand becomes discovering how best to devise controls around this access.

Fortunately, the problem is not as formidable as it sounds. Access control solutions for the network exist in many forms and products that have been successfully deployed and tested.

Controls

Having identified the vulnerabilities, let us look at the possible controls one by one:

1. Interception—Good physical access controls at data centers and offices, and physical security over telecommunication equipment can act as deterrents to interception through sniffing. As a first step, the auditor could evaluate physical security, including all the points where the communication links terminate and where the network wiring and distributions points are located. However, there are limitations to the effectiveness of such controls, especially with increasing wireless communication. The most effective control to interception is encryption. When data are encrypted, even if they are intercepted, disclosure or modification cannot occur unless the scrambled data can be decrypted. Today, there exist many methods of encryption and many combinations of its use. Encryption can be done either by the application or at the communication level by a device such as a router, switch or a multiplexer. A virtual private network (VPN) is an example of the usage of encryption to tunnel data securely over a public or shared

network. The use of digital certificates and digital signatures is another example.

2. Availability—The control to ensure availability and reliability of a network is through good network architecture and monitoring. The design of the network should ensure that between every resource and an access point there are redundant paths and automatic routing to switch the traffic to the available path without loss of data or time. Every component in the network needs to be fault-tolerant or built with suitable redundancies. Complex and widespread networks need to be monitored and managed. This is often done by using network management software. The establishment of a network operations center (NOC) with software tools and a service desk often staffed 24/7 provides this capability. Such tools provide data for capacity management. They also ensure that the networks provide adequate bandwidth to enable the data to move along without bottlenecks and with the speed required by the users and applications. The IS audit review should cover all these aspects.
3. Access points—Most controls in a network are built at the points where the network connects with an external network. These controls seek to limit the type of traffic that can come in or go out and also the origin and destination of the traffic. For example, to provide access to a web server that is inside the network to customers all over the world for placing orders, the network should accept only a certain type of traffic (HTTP) and not the kind of traffic that tries to log into the server (telnet). In another situation where a partner or vendor provides, for example, system development or maintenance services over a dedicated network from a fixed location, the network may allow traffic only from those systems with specific addresses. Such controls are implemented through suitable configuration of the rule base in a firewall and/or through access control lists in the routers. Antivirus software and intrusion detection systems can detect viruses and other malicious code at these entry points and take detective and corrective action.

In addition to being at the gateways, the strategic positioning of such control devices/software and tools at critical hosts and segments of the network can enhance security further based on requirements determined by the risk assessment. The operating systems of the servers where critical resources are hosted need to be hardened and the access controls in applications also need to be controlled and maintained securely.

Auditing Network Security

The auditor needs to obtain certain information and understanding of the network that is under review to proceed with the audit of network security. This information gathering can be done in the following steps and sequence:

1. What is the network?—The first step is determining the extent of the network. This is generally done by examining the network diagram. The network diagram is basically a map that shows all the routes available on the network. The key factor that the auditor has to worry about in the diagram is its accuracy. Large networks evolve and change constantly with changing business needs and a diagram that is not updated is useless. The IS auditor should ascertain what processes exist in the organization to update and maintain the network diagram accurately. The use of a software tool to generate this diagram ensures some degree of accuracy. In any network, there will be locations where there is a concentration of resources, such as a data center where ERP servers, mail servers, etc., are hosted and many points such as manufacturing plants, sales offices etc., from which these resources are accessed. While smaller networks may have only one such location, complex networks may have many hosting points where critical resources are located. The network diagram could also provide input on the type of devices and protocols used on the network. The network diagram and its details provide the most important input for the audit, and the auditor should keep referring to it throughout the audit.
2. What are the critical information assets in the network?—The fundamental principle of information security and audit is that protection is related to the risks associated with the assets as determined by a systematic risk assessment. The auditor needs to have a good idea of the critical assets, systems and services that need to be secured. Typically, one would want to protect enterprise systems including ERPs, mail servers and other internal applications, web servers that host applications that are accessed by customers and vendors, and the network and its components. In this context, the security and access mechanisms surrounding the applications and the servers (the OS and database) also need to be robust.
3. Who has access?—The next step is to determine the persons who have access to the systems on the network and how. Is the system accessed only by employees? Do customers and vendors also access the systems? Do employees access the system from outside the office? Do customers access only the web server via the Internet or do they perform remote logins to the enterprise systems? The answers to these questions will have significant impact on security.
4. What are the connections to the external networks?—Although this is actually a part of step 1 and is determined by a study of the network diagram, it is an important step and should be dealt with separately. At a minimum level, every network today is connected to the Internet through an Internet service provider. The primary reason for connecting to the Internet is to enable receipt and dispatch of mail and to enable browsing by employees. Enterprises may also have other reasons to connect to the Internet, such as e-commerce web sites through which the company's vendors, customers and partners collaborate, place orders or exchange other information. Dedicated connections to the networks of other partners may also exist. The gateways through which each of these connections is made are potential entry points for the external world.

The auditor could at this point try to identify the demarcation between the internal network and the external network. Based on step 2, the IS auditor would already know which systems are accessed only by internal users, which are accessed from the external world or the Internet and which are accessed only by the external users. Such categorization would also help an auditor determine the effectiveness of the design of the demilitarized zone and the positioning of security products like firewalls and intrusion detection systems. A major effort would be to secure the internal network from the external world at the gateways. This is not to say threats come only from the outside. Threats from inside are as serious as the ones from outside. The auditor needs to evaluate whether both are adequately handled. To secure systems from internal threats, all host-based security such as application and OS-level security needs to be evaluated.

5. What are protection mechanisms?—Once the basic understanding of the network, the resources and the risks has been obtained, the auditor is ready to look at the protection mechanisms. The auditor can then evaluate them for effectiveness and adequacy.

Evaluating Protection Mechanisms

The first step is looking at the gateways as the potential points through which entry can be gained by the unauthorized or malicious code. The controls are implemented through a well-designed and secure network architecture, choice of protocols and encryption mechanisms, choice and configuration of network devices such as routers, and additional defenses including firewalls, antivirus and intrusion detection systems.

Evaluating every one of these requires specialist knowledge, and the auditor would do well to ensure that the audit team evaluating network security consists of experts who have specific knowledge of the protocols, the network devices and the software deployed at the network. The focus of this article has been to sketch a basic approach to network security audit, and not to provide specific audit and technical guidelines.

Books and searches on the Internet can provide checklists pertaining to evaluating the configurations of most commonly used devices and security products. Security products are constantly evolving. Many are developing multiple capabilities and morphing into hybrid products that provide firewalling, antivirus and intrusion detection and correction all in one. Once the IS auditor is clear about the need, role and limitations of each of these, the specific knowledge about them can be acquired or hired.

It is necessary for the IS auditor to evaluate the processes associated with the management of all these security components. Configurations need to be maintained through suitable change management procedures, logs need to be scrutinized and acted upon, incidents have to be managed and learnings and preventive action documented. Good security does not come from mere investments in complex and expensive tools and software alone. It requires a capable IS auditor to review the systematic management of the security tools through well-defined processes.

S. Anantha Sayana,
CISA, CIA
is deputy general manager, corporate IT, with Larsen & Toubro Limited in Mumbai, India. Sayana has more than 13 years of experience in IS audit and internal audit in the banking, manufacturing and services industries, spanning a wide variety of applications and technical platforms. He is a past president of the ISACA Mumbai Chapter. He can be contacted by e-mail at *sas-pia@powai.ltindia.com*.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

www.isaca.org