Computer Security

By: Capt S B Tyagi, FISM, CSC

There can be little question of the importance of the computer in the business world of today, and its increasing significance in the future. Yet, in spite of the benefits to be derived from a computerized operation, it creates a great potential for danger. Probably no one element in business, including catastrophic fire and the ravages of non-computerized internal theft' presents a greater potential to wipe out an entire business so quickly and so effectively.

The dangers that can befall a computer center or can be created by it encompass virtually the entire operation of busyness it serves. Embezzlement, programming fraud, program penetration, operator error, input error, program error, theft of confidential information, and plain carelessness are a few of the problems that can arise in routine operation. Add to this the potential for fire, riot, flood and sabotage.

Increasing threats to computerized data

In the face of the risks to this sensitive machinery and to the enormous accumulation of data concentrated in the limited area, as well as business's ever increasing reliance on the computer, many firms continue to ignore the dangers. Many of them confess an-uneasiness about security for the computer but claim they cannot afford an effective protective program.

There is no question that computer security can be costly, but the stakes are too high to try to effect economies in this area. The fact is that any company involved with a computer-and that includes most companies in this country-can not afford not to have a comprehensive security program that will protect their computer operation. Since such installations can represent an investment running in to the millions of rupees, a security program costing from Rs. 50,000 to 250,000 is not an unreasonable expense.

Ideally the program designed to provide computer security will be an integrated part of the company's overall loss prevention effort. It should be administrated by a specialist in computer operation, but it will report to, and be coordinated with, the large program. It must encompass physical security, procedural or operating security, access and traffic controls, disaster planning and contingency procedures, employee education programs and a painstaking screening procedure in the employment of computer personnel.

Security measure for computer cells

Security managers must protect the corporate network without diminishing its level of efficiency. To do so, they must answer the same type of questions that pertain to physical security. These include: What needs protection? Who might attack? How will they do it? How can risk be managed?

Protecting the Network Neighborhood

WHAT NEEDS PROTECTION?

Every item with a network cable attached or connected through wireless communication is a potential target for attack and thus a candidate for protection. Web servers, mail servers, and firewalls are clearly assets that need protection. Individual workstations need protection, too, as many Internet vulnerabilities are created by actions of users. For example, all the popular Web browsers have security holes that can be exploited by a hacker to read the contents of the local hard drive; these attacks usually depend on users performing a task, such as downloading a file, without being aware of the security implications.

The network infrastructure needs protection as well. Switches, routers, even hubs can come under attack. For example, there is a standard communication method, called simple network management protocol (SNMP), that lets network managers exchange data with a network device, such as a router, to gather information about the device. A would-be attacker can take advantage of SNMP to learn how the network is configured. In many instances, an attacker may even use SNMP to change the configuration of attached devices so that the penetration can be veiled.

In highly sensitive environments, protection of the physical cabling should also be considered. If appropriate physical protections are not put in place, someone with access to a company's grounds can tap the cables and intercept the information being transmitted. This danger can be mitigated inexpensively by keeping wiring closets locked and securing the keys.

WHO MIGHT ATTACK?

The next step is to assess the nature of potential attackers. They are likely to fall into one of four main categories: hackers, business rivals, foreign intelligence gatherers, and insiders.

> **Hackers:** For most people, hackers are the first to come to mind when it comes to breaking into systems. This is a more diverse group, however, than the rubric implies. In security circles, most of these people are known as "script kiddies." These are not

programming geniuses; they don't find new and interesting ways to subvert security measures. Instead they use scripts or programs ('sploits) produced by others to break into systems that have not been patched or otherwise secured.

Most "hacks" that get reported in the news are the result of script kiddies running someone else's program against a corporate network that has not been secured with the latest readily available fixes. The hackers who are programming geniuses are generally not in the business of sport hacking, but in generating new security knowledge about the inherent weaknesses and vulnerabilities found in mass produced software and hastily secured networks.

Business Rivals: Competitors may try to obtain information illicitly through your virtual back doors. To avoid being identified, competitors may mount attacks through a third party. Because the stakes of their exploits are high, these attackers are also likely to put considerable resources into the effort.

Foreign Intelligence: Another area of concern is foreign espionage. France, Israel, and Russia are known to have active industrial espionage efforts underway against the United States. Other suspected countries include India, Germany, and Japan. As with a competitor, foreign spies are likely to bring substantial resources to bear in obtaining information. They are also likely to use tactics that require more time, such as placing an employee within the company.

Insiders: While outsiders present a daunting challenge to corporate networks, the Computer Security Institute reports that outsiders--people without any legitimate access--account for fewer than half the reported information security incidents in the United States, although their numbers continue to rise. The majority of incidents occur at the hands of people with some degree of legitimate access, ranging from employees to former employees, customers, and contractors.

Insiders may fall also into one of the prior categories; they may be hackers for their own amusement, for example, or they may be working for rivals or foreign intelligence agencies. They may also be former insiders who take advantage of their knowledge of the system to retain access to the network. In some cases, they may simply continue to use access privileges that the company failed to terminate at the end of their employment.

For example, one company conducting security audits discovered that an employee who had been terminated 18 months earlier had continued using his network account to distribute pirated software. Regular system administration should have included disabling the user accounts of departing employees.

HOW ATTACKS WORK:

No matter who the attackers are, they try to enter the network to start an attack in the same way: by probing for information and locating IP addresses, services, and sources of more information. For example, they may use a tool that sends out signals to find out if the company uses FTP (file transfer protocol, a service for remote transmission of files). They will then try to determine whether the FTP service offers an easy entry point--for example, if it allows root access through guessable user names and passwords.

Publicly available information, such as a company's Web site address, can provide clues about access to the rest of the network. Freely available utilities will identify a company's Internet service provider, probe DNS records, and find targets for more invasive probes.

Finding Holes:

Once a target has been identified, the attackers can employ freely available toolkits that find and exploit a wide range of problems. For example, if a telnet server (another network service for remote connections) is found, software can automatically try a series of default user name and password combinations to see whether login is available. If a Web server is found, programs can test it for hundreds of known bugs and security glitches. If a mail server is found, a script can illuminate dozens of problems that could let an outsider gain access.

There is several freeware security scanning suites that will assess a wide range of security problems. Tools such as Nessus, nmap, SATAN, and mscan all check for many potentially exploitable problems. An attacker can easily obtain one or more of these tools and run them against a range of IP addresses. Overnight, the attackers can generate a list of security issues on hundreds of computers. At their leisure, attackers can use the list to probe more deeply and perhaps actually exploit a few of the problems to gain access to the targeted systems. (A standard countermeasure is for systems managers to run these tools themselves to see what results they obtain.)

Would-be attackers may also begin their search for network vulnerabilities in the physical world. They may, for example, look in dumpsters for un-shredded documents that contain company phone lists with e-mail addresses that are also user names. Hackers are also fond of using "social engineering" techniques to get user names and passwords. The con works by convincing an unaware employee to divulge his or her password or other security-related information.

Covering tracks:

Once attackers have a preliminary foothold, their next step is to cover their tracks. For example, Rootkit, a Unix and Windows NT software package, erases logs, installs system utilities that cloak hacker activities, and opens a backdoor to the system so they can return. Now the system can be probed by the attacker for information, or it can be used as a platform to attack other systems.

Attacking from within:

As mentioned, insiders account for most security incidents. Insiders with malicious intent usually attack in precisely the same way as outsiders. Since they are already in the network, insiders can mount extremely effective attacks with minimal effort. Without appropriate safeguards, such as detailed access restrictions, a company is wide open to insider abuse.

Systems administrators already have privileged access to their systems and can use that access to attack other systems while completely covering their tracks. Regular users can promote themselves to administrative users with minimal effort. There are many free utilities that rarely leave an audit trail that convert a regular user to a privileged user.

HOW TO MANAGE RISKS

Once systems managers understand the company's exposures and threats, they have a good idea of the specific risks that must be managed and mitigated. They must now find ways to balance the need for security with usability. The most effective approach is to collaborate with business managers, senior management, and technical staff.

POLICY

The purpose of an information systems security policy is to communicate that information security is a priority to the company and that everyone is responsible--and accountable--for maintaining it. The policy should define the information that needs protection and delineate which measures--technological and procedural--are in place to do that. It should, for example, explain how incidents should be reported, what records should be kept, and what the response will be. The policy should also describe what is expected of each group of employees (staff, managers, etc.) with regard to achieving the goals.

In addition, the policy should define acceptable behavior as well as disciplinary guidelines for infractions. It should state privacy standards. Furthermore, the company should set forth measures for staff to follow so as to limit the potential for future liability arising from the handling of electronic data. For example, if the company electronically exchanges information

with business partners, employees must be advised about inappropriate disclosures of sensitive third party information.

The policy must also support the organization's business objectives. Otherwise, management will not support it. In this regard, as mentioned earlier, collaboration with other business units who will have to buy into the policy is critical. For example, I consulted with a company planning to deploy a new authentication mechanism for its remote sales force. Security planned and implemented the scheme without consulting the users or their management. When rollout arrived, the sales force rebelled and refused to use the mechanism, complaining that it was too difficult. The dispute quickly escalated, and the security staff lost the ensuing battle. After all, the sales force brings in the money and must be able to do its job. Security succeeded only in wasting time and money, and ultimately effected no security improvement. Eventually, this organization initiated a more collaborative process and arrived at a solution that satisfied everyone.

Controlling privileges. An important component of network protection is proper oversight of user privileges, which should be complemented by a layered defense designed to prevent those with limited privileges from easily gaining access to restricted parts of the network. The obvious place to begin separating privileges is at the borders of the network. The system administrator should regulate each user's rights and permissions with regard to file access, placing the appropriate security measures, such as additional login requirements, at particularly sensitive areas. The security manager must remember that every group will have some degree of privilege, the minimum most likely being the general public's right to view the Web server and send e-mail. At the high end of the privilege scale are system administrators. In between are users with varying degrees of authority.

The key is to carefully delineate user privileges. If users have only the minimum privileges required doing their job and responsibilities are separated within the network, it will be difficult for a disgruntled employee to get very far.

Permission and access rights should be "fine-grain," or specific to individuals, departments, and processes. For example, research and development probably should not have access to the network used by human resources, and neither should they be able to run accounting systems. Most network operating systems come with these configuration capabilities.

Layered defense*.* If information has to flow inward from the Web server, as is often the case, there is at least one potential hole through the perimeter defense. Likewise for e-mail, the messages need to get to the internal users at some point, and that means a malicious mail payload may get through as well.

A well-designed perimeter defense will, therefore, minimize, but not eliminate, potentially damaging inbound network traffic. Other layers of protection must also be deployed, including for the Internet, for network links to remote offices, and for remote access points such as modem pools and extranet connections.

Auditing Traffic. Putting privileges and layered defenses in place will not stop all hacking attempts. Therefore, it is also essential to examine audit logs regularly. Most operating systems and software packages have logging capabilities that should be enabled to catch important events and aid in forensic efforts.

Tools for Defense:

No security operation is complete without regular use of security tools that help system administrators do their jobs more efficiently and improve the overall security of the network. Still, no tool is a complete remedy, and each tool's limitations must be recognized.

Firewalls: Firewalls are an essential component of any perimeter security strategy. They are the basic building blocks of restricting network traffic, such as between the Internet and the internal systems. Less often considered is that firewalls are also good for segmenting internal networks. A firewall lets a system administrator separate functional groups, while still permitting required traffic between the areas. It can also provide an audit trail of authorized and blocked traffic, which may allow staff to spot probe attempts or other unauthorized activity.

Firewalls, however, by no means create total security. By their nature, they must allow some traffic through, and that traffic may become an attack vector. They can also be bypassed. Dialup lines may provide backdoors, as might WAN circuits.

VPNs: Virtual private networks provide transmission security--protection from passive observation of a data stream and from insertion attacks (where the attacker injects information into an established data stream). Generally, VPNs are used for remote offices and nomadic users who require access to sensitive information such as e-mail.

The primary pitfall is forgetting that the endpoints of the VPN must be secured. For example, if an authorized user's laptop is stolen, anyone possessing the laptop will have free access to the VPN unless a strong authentication mechanism is in place. VPNs don't replace any other security measure, but they do make a solid contribution when secured properly.

Hacker tools: Software such as security scanners or vulnerability assessment tools are intended to help system administrators view their networks from an attacker's perspective so that corrective action can be taken. For example, some programs will scan a network to see if it is vulnerable to any number of current holes. Others attempt to crack passwords, which will alert security if employees are selecting words that can easily be guessed. However, like

antivirus software, these tools are only as good as their last update. Most vendors of these packages update fairly frequently.

None of these packages will find everything, so it is wise to use a combination of these tools, such as nmap, SATAN, and Crack. To get the best results from them, administrators must update and run these programs on a regular basis, and their reports should be examined closely.

Intrusion detection: Intrusion detection systems (IDSs) detect malicious activity either through listening to the network wire or by monitoring logs. They compare the activity flagged to an internal database of attack signatures. In practice, IDSs, like anti-hacker software, are only as good as the last update of the database. IDS technology is still quite immature and cannot be thought of as a cure-all.

People: It is important to remember that security is not just a technical problem. Technology plays a big part, but it is only one piece of the puzzle. Ultimately, people are the most important piece.

As we have seen, nearly everyone has to be involved in policy development and implementation. One group deserves special attention, though. The system and network administrators who have day-to-day operational responsibility must also be security-aware. This group has the ability to make or break any security measure because they are the ones configuring and re-configuring the systems that have to be secured. They have their eyes on the machines and on the wires every day.

Several important ingredients help substantially in creating a security-positive administrative staff. First, and foremost, is priority. From their first day on the job, system administrators should be told the importance of a secure environment. And that message must come from the top.

Basic training in the tools they need for security is also in order. Additionally, administrators need to know what constitutes a security event and what to do about it. The company's information policy should identify what constitutes a security incident, and it should have clear criteria for incident handling.

In addition, as mentioned, the general employee population will need to be in the loop. From orientation onward, employees need specific training and frequent reminders of their information security responsibilities. For example, they should know the security and legal ramifications of copying software, downloading from the Internet, bringing disks from home, and divulging sensitive information. They should know how to create and protect passwords, be aware of social engineering, and know how to report incidents. The technical staff imparting

all this knowledge should not forget how complex networking could be. They should make sure that procedures are explained in plain English.

Commonsense approaches to building, implementing, and maintaining a security policy will go a long way toward fortifying a company's information sanctuary. By combining good general security practices with the right high-tech tools, companies can make sure that their information will not be an easy mark.

***

NETWORK SECURITY STATAGY

By: Capt S B Tyagi, FISM, CSC

Computer networks are operating in an increasingly risk-prone environment. Hackers, competitors, dishonest data brokers, and disgruntled employees have a seemingly endless menu of attacks to choose from these days. Companies can build their computer system's defenses just as they would strengthen their body's ability to ward off infection--by developing a regimen of "healthy" practices and sticking to it.

The following steps are recommended as a guide to consultants or in-house information systems (IS) security professionals who are called on to secure a corporation's network. These steps can help management ensure that the proper computer security policies and procedures are put in place and that they are followed by all employees.

Develop principles.

The company should first develop an official IS security policy with guiding principles that communicate corporate security objectives. This policy serves as the foundation of the organization's security infrastructure. Principles should be developed with input from information systems personnel or other personnel responsible for any portion of the information stored on the network. They must also receive the full support of senior management. In addition, the plan should serve (not hinder) the overall corporate mission.

The policy should include a discussion of computer security responsibilities, penalties for noncompliance, and classification of information. It should also address viruses, physical security of network components, telecommunications security, and Internet and remote access. In addition, it should include procedures for network intrusions, laptop security, and data backup and restoration.

> ***Responsibilities.*** This section gives employees specific instructions on their roles in protecting the network. For example, the policy can explain the importance of safeguarding passwords and never giving them to anyone under any circumstances.
>
> It is also a good idea to include a passage on social engineering, a technique used by outsiders to obtain information from unsuspecting employees. A hacker, for example, might call claiming to be a technician working on the network who needs the employee's password. The policy should tell employees what to do if they receive such a call; for example, the policy might require notifying IS personnel.

Penalties. As the old saying goes, the punishment must fit the crime. If the company is serious about network security, it must be ready to mete out penalties to those who violate policy, but penalties must be reasonable.

Classification. Information should be given a confidentiality rating based on the damage that would result if it were lost or stolen. The policy should state how these ratings are to be assigned and who can access the information in each rating category. It should explain where on the network classified information should be placed and whether additional safeguards are needed.

It is a common practice to divide the classification into levels from zero to five, depending on the impact that will result should the information be disclosed, altered, damaged, or deleted. Zero would signify no impact, while five would represent a catastrophic impact. For example, a personnel database, the corporate five-year plan, and executive e-mail messages would be level five, basic public information level zero.

Viruses. A proviso should explain the devastating effects of viruses. Employees should be made aware of how they may inadvertently bring viruses into the network, either through their online activity or by transferring disks between home and work. In companies where there is a great deal of proprietary information being stored on the network, some policies bar employees from bringing any diskettes from the outside. Others require that any disk brought from external sources first be scanned by an antivirus product before use on company machines.

Physical security. In general, the policy should require some physical security to protect the servers or mainframes that store and transmit all the company's sensitive data. At a minimum, the policy should require that they be kept in a separate room that is locked and requires key or card access. Only essential personnel should have access to this room.

Because most workstations are located in the open in employee cubicles, physical access controls in the sense of locked doors are not practical. However, some companies require the use of special cable lockdowns at the end of each workday.

Telecommunications. Many corporations have incorporated PBX / telecommunications security into the duties of information security because telephone lines are used to connect individuals and transmit data. The corporate security policy would state that telecommunications security is the responsibility of those charged with information security or, if separate, that the groups work closely together.

Internet and remote access. If Internet use is allowed within the company, the policy should call for a firewall as a minimum security measure, and possibly a system of

routers with strict access control lists that designate what data can get in and where the data can go on the network. The policy should designate responsibility to at least one IS employee to maintain the lists and ensure their accuracy.

The policy should also be extremely cautious with remote access. No general employees should be allowed to circumvent the network's firewall or other protections by setting up an internal or external modem on their computers. Doing so could permit an outsider to gain access not only to that computer but also to the entire corporate network.

However, it may be necessary for some executive staff or key network engineering staff to have individual modems. In this case, security should ensure that all communications via these channels be encrypted. IS personnel should install one of several security tools available to keep remote access secure. For example, some tools offer a call-back feature in which the employee dials in, authenticates to the system, and is then disconnected after the system identifies the phone number from which the remote executive is calling. If the number is on a pre-approved list, then the system calls the remote computer back and initiates a session. Other products offer different approaches, such as challenge-response techniques, biometrics, and virtual private networks; these should be reviewed and selected based on what is most practical for the company.

Network intrusion. Among the most common defensive tools being implemented on computer networks today are intrusion detection systems (IDS). Generally, when evaluating these systems, the security manager should be looking for those that automatically alert IS personnel via pager, e-mail, telephone, or console to potential intruders into the network domain. The intrusion detection system should provide "exception" reports when something out of the ordinary occurs. The security manager should devise a plan of action for information systems personnel to follow when they've been alerted to a possible attack or unauthorized activity on the network, such as shutting down the connection and reporting the incident to their manager.

Laptops. Laptops require special attention because they are one of the hottest commodities companies have around. The policy should stress employees' need to monitor the whereabouts of their laptops, especially when on travel. The policy might state, for example, that employees must keep the computers in their possession at all times or in a secure place such as a hotel safe.

Companies might consider using a laptop tracing service, in which the computer periodically calls a monitoring service, whose representatives can track its location. These services have led to several successful recoveries. If this type of service is used, the policy should make employees aware of it.

Backups. This portion of the policy should explain how information is backed up and how often. For example, it could state that a full backup will be performed once a month, while a nightly backup would save only newly modified files. It should state how long files will be stored, explaining clearly the conditions under which employees who have lost data will be able to retrieve it.

Know the layout.

The security manager also needs to understand what is called the topology of the network. Topology focuses on the structure of the network that provides the interconnection among nodes. Topology charts the location of each machine, each connection, and all devices that make up the network.

The security manager should examine this organizational infrastructure, noting the current configuration with an eye toward security holes and performance issues. Among the items to be inspected are cabling and wireless equipment.

Cabling. The security manager should look at the type of cables, such as 10baseT, shielded, or fiber optics, that are used to connect machines. Security risks are associated with each of these. For example, many companies have fitted their facilities with fiber optics because the technology was considered more secure than regular cables. However, I have found that if bent at the proper angle, data is no longer contained within the cable fiber, and with the right instruments, one can stand outside the company's walls and intercept data being transmitted. The security manager should, therefore, understand the potential vulnerabilities of each type of data transmission technology being used and conduct regular inspections to ensure that these vulnerabilities are not being exploited.

Wireless equipment. Security managers should not neglect the increasingly popular wireless devices that access the network. More companies are using equipment such as palmtop computers that transmit data through infrared, microwave, and radio frequency (RF) technology. For example, retail companies might find the hand-held technology useful in plugging inventory data from the warehouse floor right into the network. However, the network security manager should be concerned about preventing this data from being intercepted.

To minimize the risk of interception, three popular techniques can be used, including spread spectrum, frequency hopping, and encryption. Spread spectrum involves transmitting data over several frequencies. So, for example, if someone managed to intercept the data on one frequency, the person would only get a fraction of the information. Frequency hopping calls for the changing of channels periodically during each transmission to elude intruders. The third

option is to use software that encrypts data so that anyone intercepting the message would see only meaningless bits and characters.

Assess awareness.

The security manager should next talk with employees to assess how well they know the system and their roles and responsibilities in keeping it safe. I have found that it is best to tailor questions to be answered with yes, no, or other short responses so that information can be analyzed quickly and with little room for misinterpretation. I also recommend conducting most interviews one-on-one. In groups, some employees may be afraid to speak up on crucial issues.

All information systems security staff, system administrators, technicians, data owners, end users, and line and senior management should be interviewed. The survey results will help determine whether any procedures should be adjusted or whether additional staff training is needed.

> ***IS security team.*** Information systems security staff members should be asked whether they feel supported by management. In addition, the security manager will want to ask whether the team is regularly included in new projects that involve the network. The IS team should be included at the beginning of these projects, and at least one member of the staff should be included in the project through completion. Further, the security manager should ask team members whether other computer-related personnel such as system administrators, network engineers, and technicians follow the security-related instructions, policies, and procedures they set.
>
> Next, the team should be asked to explain the security tools, such as firewalls, routers, intrusion detection systems, and antivirus solutions that are in place to protect the network. IS employees should be asked to speak candidly about how well they are trained to operate each tool. The interview should also reveal how often audit logs on all systems are reviewed and how the team finds out when there is a problem with the network. This information can help management assess whether reporting procedures are being followed.
>
> The interviewer should then review the network diagram and ask the IS security team members whether they know of any security flaws or performance bottlenecks that exist. The interviewer should pay close attention to the interviewee while reviewing the diagram. He or she will want to look for indicators that the interviewee knows the system well. Curt or incorrect answers, as well as those that evade the questions, should raise red flags and signal the need for more experienced personnel or more extensive training.

Administrators and technicians. As with the IS security team, system administrators and technicians should be asked whether they believe they receive enough support, such as the needed funding to properly manage the network. In addition, the security manager should assess this group's relationship with other personnel, its level of training, and its knowledge of network operations.

Data owners. Data owners are personnel responsible for some information on the network. A common term in the insurance industry, it may designate personnel such as claims managers who frequently access claims. A human resources manager might be considered the data owner of a personnel database.

Data owners should be polled to find out whether they believe their data is being properly protected, why they feel as they do, and whether they have experienced data damage or inaccessibility. The interviewer should ask data owners whether they meet with security personnel to discuss data protection and whether they include system administrators in those meetings or in other meetings that involve network issues.

End Users. The general employee populace should be questioned to ascertain their level of security awareness. In the interest of conserving time in larger companies, an anonymous questionnaire may be distributed for this portion of the interview process. Employees should be asked whether they have read any existing corporate security policies and whether they generally adhere to them.

In addition, the interviewer should ask about common security concerns. For example, does anyone else know an employee's password? Employees should be questioned about their remote access activities as well.

Senior / middle management. The higher ranks of corporate management should be asked whether they support the security policy and whether they adhere to its provisions. The interviewer should also ask whether anyone else knows their passwords, whether they remotely access the network, and whether they believe their corporate data is being properly secured.

It is particularly important that senior management adhere to policy, because they set the example for other personnel. In addition, they access the most sensitive information, such as bids, proposals, and plans. They should be polled further to see whether they know of any existing flaw in the network. They should also be asked to comment on whether current security policies and procedures interfere with any corporate business objectives or goals.

Should this portion of the survey reveal that executives are not following policy, I have found it helpful to show management reports of cases in which corporations have suffered financial penalties from lawsuits due to improperly secured networks.

Manage change.

The security plan should assign an individual or group in the company to be responsible for managing change. Before changes are made to the corporate network architecture (hardware, software, or preexisting policies and procedures), the security manager needs to work out a framework through which these alterations will be handled. Any modifications should be agreed to by all appropriate parties. Approved changes should be properly documented in network diagrams.

Audit systems.

Each machine should have maximum security to the degree that it does not significantly impede required network performance. The specifics of how to audit a system vary based on the type of operating systems being examined. However, several overarching items should be included in any audit.

First, the security manager will want to make sure directory and file permissions are correct--that the system is granting only authorized users access to files and directories, and that it is allowing them to perform only authorized actions, such as reading, modifying, copying, or deleting. The audit should also determine whether employees are complying with password policy regarding length and other security requirements.

Analyze risk.

A risk analysis is a comprehensive study of the entire network. Risk analysis provides a systematic approach for understanding the total network security posture. When performing a risk analysis, the security manager should document the network if this hasn't already been done, place a value on information assets, identify vulnerabilities and threats from within and without, and then choose the most cost-effective strategies for implementing safeguards.

As part of a client project I was involved in, for example, an intrusion detection system was installed and over a period of a month, nearly forty intrusions were detected. The installed tool then helped to shed light on numerous vulnerabilities the organization was facing, such as the sending of e-mail passwords "in the clear," or unencrypted, over the network.

Effect Safeguards.

The next step toward sound security is installing any security tools for which the risk analysis revealed a need. These additions to the network should be documented and agreed to by management. In addition, all tools need to be tested to ensure that they are configured properly, work as planned, and do not introduce new security concerns.

Test constantly.

In addition, security managers should have system security tested on a regular basis to ensure that security constantly adapts to new challenges. One of the most popular ways to do this is through penetration testing in which consultants or in-house personnel, using their own knowledge and various software tools, imitate the course of action a hacker would take when attempting to break into the network. The testing can be done across the entire network or, as is more often the case, on specific information resources, such as firewalls, routers, and servers, that have been designated as critical to the company.

Train.

No security plan is complete without provisions for ongoing awareness training. Employees, vendors, and contractors can make or break the security of your network, and they should all receive computer security training when hired and at least annually. The training should explain the reasons for security and ensure that everyone fully understands his or her responsibilities.

Respond.

Because no amount of planning and technology can completely insulate a company against an attack, network security must inevitably include procedures for handling computer crime. One step to take well in advance of an actual incident is to set up the proper contacts in law enforcement and find out how to legally gather evidence related to a computer crime. These steps will greatly increase the chance of a successful prosecution should a company choose to go that route.

In addition to having clear procedures for criminal investigations, the company may want to establish a crisis management team within the IS department. These staff members will have special training on how to respond quickly to an incident, how to immediately recognize its potential severity, and how to handle evidence and work with law enforcement on a case. The team should also be trained to explain to law enforcement the various types of security measures, such as auditing tools, that were used to trace the connection of the perpetrator and examine his or her activities.

There should be a procedure that outlines what to do if the system has been compromised and the intruder is still in the system. For example, the policy might call for the on-site administrator

to immediately shut down the intruder's connection, log the incident, and contact senior personnel. Conversely, the policy might call for the system administrator to leave intruders on so that security can monitor their actions and find out what they are after or what holes they are exploring. Some companies even set up phantom servers to fool intruders, which may help security trace their path or feed them false information without putting the network at risk.

In devising and maintaining a sound network security strategy, management must remember that security is a dynamic process. As new and more complex challenges emerge, security measures must be modified. A regular security regimen that helps IS constantly reevaluate the effectiveness of policies and procedures can go a long way toward keeping security robust and ready for the inevitable attack that will be mounted against the system's defenses.

*****