SECURITY

Best Practices For Securing Enterprise Networks

David M. Piscitello and Lisa Phifer

There are no short-cuts or cookie-cutter approaches, but there are concrete steps that can tighten your network security. Do you have the will? Can you get the resources?

Information is the lifeblood of any business. Enterprise networks sustain the vital flow of data between employees, business units, customers, suppliers and partners. Cyber attacks interrupt or misdirect corporate information, with potentially serious consequences for the victimized company.

Few would argue against networking a company's information assets. Enabling communication with and between business systems increases operating efficiency and creates revenue opportunities. Safeguarding networked assets is therefore an operational *and business necessity*, but to do so, you must understand the threats, quantify the potential cost of being attacked and employ security best practices to manage business risk.

Attackers: Who And Why

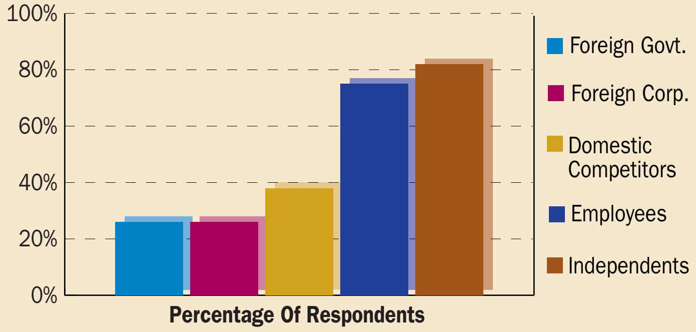
According to the 2002 CSI/FBI Computer Crime and Security Survey, an overwhelming 90 percent of the companies surveyed detected security breaches last year. Nearly three-quarters (74 percent) had experienced Internet-based attacks, a doubling in the past six years. In 2001 the number of security incidents actually reported to law enforcement topped 50,000; by mid-2002, the number of reports had already exceeded 40,000. Empirical evidence therefore makes it very clear that cyber attacks are growing.

But just where is this threat coming from? Most attacks are launched by what the FBI calls independent or "non-motivated" attackers—miscreants and criminals who try to penetrate your networks and systems for fun, notoriety and fame. Many take pride in being members of a "cybercrime" underworld where they brag about conquests, debate attack techniques, share exploits and exchange intelligence about vulnerable targets. Perpetrators include knowledgeable "script kiddies" and "ankle biters" who simply download attack tools and use them in obvious ways. More worrisome are attacks by disgruntled employees and computer terrorists, while independent attackers and company insiders constitute the biggest threats, preying on the vast majority of companies surveyed by CSI (Computer Security Institute—see Figure 1).

Why do they attack us? Most attackers are computer-savvy teens, out to impress peers, flaunt authority and earn notoriety under the dubious banner of hacktivism. They seek out vulnerable systems with little regard as to the owner's identity or consequences.

On the other hand, competitors commit corporate espionage by selectively and surreptitiously stealing trade secrets, marketing plans and customer data. Disgruntled employees have a different goal: To damage, destroy and disclose

FIGURE 1 Likely Sources Of Attack (2002)



Source: CSI/FBI 2002 Computer Crime and Security Survey

David Piscitello (dave@corecom.com) and Lisa Phifer (lisa@corecom.com) are, respectively, president and vice president of Core Competence, Inc., an internationally recognized consulting firm specializing in network security. David also is the founder of the Internet Security Conference, and has chaired the N+I Conference Program since 1996.

Table 1: Top Ten Windows Systems Vulnerabilities

1. Microsoft Internet Information Services (IIS) fails to handle unanticipated requests and buffer overflows, plus breach through use of sample applications.

2. Flaws in Microsoft Data Access Components (MDAC) Remote Data Services (RDS) allow remote users to run commands with administrative privileges.

3. Microsoft SQL Server vulnerabilities allow attackers to obtain sensitive information, alter database content and compromise SQL servers or hosts.

4. Improper configuration of Windows Networking Shares may expose system files or let attackers take control of the share host.

5. Null Sessions (Anonymous Logon) can be exploited to retrieve user and share names or connect without authentication.

6. LAN Manager Authentication password hashes are stored by default and can be easily cracked using brute-force attack methods.

7. Windows user accounts without passwords or with weak passwords can make it easier for attackers to gain system access.

8. Multiple vulnerabilities in Internet Explorer, including page spoofing, ActiveX control and scripting CVEs, MIME- and content-type misinterpretation, and buffer overflows.

9. Remote registry access creates a vector through which attackers can compromise a system, adjust file associations, or run malicious code.

10. The Windows Scripting Host (WSH) permits any file ending in ".vbs" to be executed as a Visual Basic script, creating a vector for worm propagation and malware execution□

Too many organizations fail to keep current on software patches

sensitive data, thereby crippling or embarrassing the victim. Cyber-terrorists wreak havoc in public forums, defacing websites and disrupting business systems to make political or social statements. Recent public attention to Homeland Defense and cyber-security reflects the U.S. government's increased concern that terrorists may target critical public infrastructures through cyberspace (the White House's draft strategy document is available at www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf).

CyberWarfare 101

Internet connections are the most oft-exploited attack avenue, but certainly not the only vector. Insider attacks frequently originate from internal systems or remote hosts dialed directly into access servers. Virtual private networks (VPNs) that expand the Intranet to include teleworker, traveler and business partner systems represent additional entry points.

To invade networked resources, attackers begin by identifying potential targets. They use DNS and WhoIs to query public databases, obtaining addresses and hostnames. They scour websites, mailing lists and press releases to find or guess locations, servers and employee identities. Attackers turn this seemingly innocuous public data against you, using pings, port scans and discovery tools to systematically map out your network, identifying key routers and servers.

Once attack targets have been discovered, commercial shareware and hacker tools can be used to exploit listening applications, weak access controls, improperly configured services and known software vulnerabilities. Each compromised system becomes a springboard for further attack, penetrating deeper into your network or even using your assets to launch further attacks against others.

Most cyber attacks exploit "CVEs"—common vulnerabilities and exposures. Responsible vendors usually release patches to close loopholes shortly after discovery, but many organizations simply do not keep up with these patches. Attackers leverage this common oversight to take the path of least resistance to compromise your systems.

The most frequently exploited CVEs are present in commonly-used Windows services like IIS, SQL Server, NetBIOS file sharing and Internet Explorer (see Table 1; visit www.sans.org/top20 to view a Unix list). CVEs like these are the result of poor security design, inadequate testing and errors introduced by maintenance updates. Other vulnerabilities are the result of operator error, improper use or lax security practices. For example:

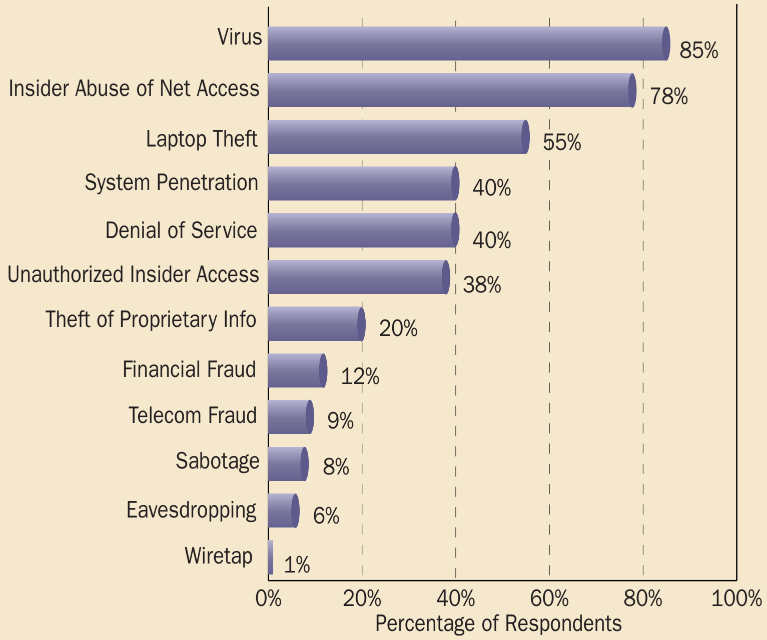
- Disclosure of logins and passwords through social engineering.
- Default or sloppy configurations that leave loopholes for attack.
- Unused servers installed by default and never disabled or removed.
- Inadequate inbound traffic filters that permit outsider attack.
- Open outbound ports that can be exploited by trojans and zombies.
- Weak CGI script and form input checking on Web servers.
- Failure to use file system permissions to deter unauthorized access.
- Lax logging and data archival practices.
- End user failure to keep A/V protection up to date.

Start by conducting a thorough risk assessment

- Execution of virus-laden email attachments.
- Unfettered use of peer-to-peer applications like Kazaa and instant imaging (IM).
- Weakly authenticated network management agents.
- Wireless LANs with inadequate access control or confidentiality.

According to CSI, the most frequently reported security incidents last year were virus infection, insider abuse of network access privileges and laptop theft, system penetration by outsiders and denial of service (DoS) attacks (Figure 2).

FIGURE 2 Types Of Attack Or Misuse (2002)



Source: CSI/FBI 2002 Computer Crime and Security Survey

Risky Business

When attackers manage to breach your network and system defenses, consequences can result in both direct and indirect financial impacts.

- **Cleanup and service restoration** due to business systems damage. According to Computer Economics (www.computereconomics.com), the worm virus Nimda infected over 2.7 million systems in just 24 hours; the recovery and downtime cost: $653 million. Meanwhile, CSI says that the system penetrations reported last year resulted in an average loss of $115,000 per respondent.
- **Business disruption** caused by loss of mission-critical data and system/network downtime during the attack and recovery period. According to Cahners In-Stat, a one-hour network interruption costs the average business $125,000.
- **Legal liability** resulting from theft of confidential information, involvement of your systems in attacks against others or violation of laws. According to CSI, theft of proprietary information has the most serious financial impact, with an average cost of $6.5 million per survey respondent reporting such theft.
- **External audit and network forensics investigation** to identify the point of attack, deter future attacks and prosecute the perpetrator(s). For example, an attacker who broke into an Internet banking and bill payment server in 2001 was paid $10,000 to prevent him from publishing customer data. Officials tracked the attacker to an IP address in Moscow and prosecuted him, which raised the bank's total financial damage to $250,000.
- **Loss of consumer and shareholder confidence**. The primary reasons that just 34 percent of companies experiencing attacks report them to law enforcement are fear of negative publicity and worry that others will use bad press for competitive advantage. Soft damages can be hard to quantify, but here is one example: Distributed denial of service attacks against Yahoo, CNN, eBay and several other commercial websites in February 2000 caused over $1 billion in market capitalization losses in just a few days.

The frequency and impact of network-borne attacks can be difficult to quantify. Some argue that surveys over-state loss, because those who participate are more likely to have been attacked. Others argue that security incidents and related damages—especially indirect damages—are, by their very nature, widely under-reported. Either way, there is ample evidence that the threats are real and the costs are high; you should be highly motivated to defend your company's networked assets from attack.

Where To Begin

As obvious as it seems, the way to begin to improve your security is by conducting a thorough risk assessment, which will identify your electronic assets and their value to the organization. Assets include mission-critical business systems, as well as copyrighted and patented intellectual property, research and databases containing personal or confidential material. If loss would cause you financial harm, expose you to embarrassment or legal action, or inhibit or damage your ability to operate your business, then the associated data is an asset. To any enterprise that conducts a meaningful part of its business electronically, *availability* is also an asset (or rather, loss of availability is a liability).

TABLE 2: Example Of Security Policy Guidelines

“The NAS Systems Division computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a NAS Systems Division computing system. Information is considered ‘classified’ if it is Top Secret, Secret and/or Confidential information which requires safeguarding in the interest of National Security.

“Users are responsible for protecting any information used and/or stored on/in their NAS accounts. Consult the NAS User Guide for guidelines on protecting your account and information using the standard system protection mechanisms.

“The NAS Systems Division computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a NAS Systems Division computing system. Information is considered ‘classified’ if it is Top Secret, Secret and/or Confidential information which requires safeguarding in the interest of National Security.

“Users shall not attempt to access any data or programs contained on NAS systems for which they do not have authorization or explicit consent of the owner of the data/program, the NAS Division Chief or the NAS Data Processing Installation Computer Security Officer (DPI-CSO).

“Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

“Users shall not share their NAS account(s) with anyone. This includes sharing the password to the account, providing access via an .rhost entry or other means of sharing.

“Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

“Users shall not make copies of system configuration files (e.g. /etc/passwd) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.” □

Source: Excerpt from the Acceptable Use Statement for NAS Systems (NASA Advanced Supercomputing Division) Computing Resources, www.sans.org/newlook/resources/policies/item2.pdf

For your security policy, solicit input from legal, accounting, auditing, personnel, business units and IT

Risk assessment can be a very complex process, and it’s important that you have credible valuation of assets should you seek financial restitution following an attack. Hire certified outside security auditors to perform a risk assessment or review guidelines established by organizations like the Information Systems Audit and Control Association (ISACA—www.isaca.org) before you pursue this yourself.

■ **Security Policy**: Every organization should have guidelines that identify valuable or sensitive assets, describe appropriate use and handling and define what constitutes authorized access. A security policy identifies threats to an organization’s assets, measures taken to mitigate or reduce these threats and a process for responding to attacks or security *incidents*. It also identifies conditions that necessitate escalation, disclosure and notification of law enforcement, public relations and legal counsel. In effect, a security policy says, “Here are the assets we value, how we intend to protect them and what we will do if they are ever lost, damaged or attacked.”

Few security activities are as routinely overlooked and discounted as security policy development. Without guidelines on which to base security measures, organizations lack a comprehensive strategy for protecting assets, and so make *ad hoc* and technology-driven decisions.

As a result, organizations deploy security measures that don’t adequately protect their assets. Too few employees will know, appreciate and consequently comply with security and acceptable use policies (AUPs). Lacking policies, an organization cannot be prepared to react to an attack, and will have little or no basis to hold insiders or attackers accountable for their actions. Responding to security breaches and taking remedial action will be challenging because action plans don’t exist.

To develop a security policy for your company, engage representatives from legal, accounting, auditing, personnel, key business units and IT to provide input. The expertise these parties provide is valuable: A security policy must consider an organization’s liability, accountability and business objectives.

When you have completed your security policy, have all employees acknowledge their responsibility and accountability to the policy, then consider implementation. In most situations, the time, talent and expense you invest up front to audit your network and to develop a security policy provides a meaningful return on investment, because it is more likely to comprehensively address security requirements than the alternative of “throwing technology at the problem.” For an example of policy statements, see Table 2.

Layers Improve Security

For several decades, physical security and strong perimeter enforcement were deemed sufficient for securing the wired LAN environments of large enterprises. Firewall systems at interconnection and Internet access points protected, in turn, mainframes, minicomputers and client-server LANs. These measures were even deemed adequate for e-merchant and extranet servers participating in the World Wide Web, so client and server security often received nominal attention.

This traditional security design is analogous to a soft-boiled egg: hard on the outside, soft in the middle. And, over time, the traditional design has proven entirely ineffective.

First, it's increasingly difficult to identify what is "outside," and physical security is not completely under your control. For example, organizations have an increasingly mobile workforce; when assets are "on the road," they're out of your control. Mobility extends your perimeter and eventually breaks it. Similarly, the storage of sensitive information may be localized to client computers, also not under your control.

Moreover, in the interests of B2B and B2C, organizations open access to internal servers, punching holes in security perimeters. The resulting "perimeter" becomes just as problematic to defend as a castle with an unfinished outer wall. Today's threats are more diverse and numerous than ever before, and organizations must move security measures close to the assets (servers *and* clients) they protect.

So, rather than thinking about Internet security in terms of an egg, think of it as an onion; peel off one layer, and you find another, and another…. The same should be true for your network security measures.

This strategy is often called *defense-in-depth or layered* security. The term "layered" has two important and applicable interpretations. The first is where one creates concentric rings of security services around assets. The second is to implement security measures, where appropriate, at each network layer—physical, link, Internet, transport and application. For example:

- Picture a Web server farm protected by an Internet firewall, a server intrusion detection system and file system integrity measures. If the firewall is breached, the IDS can detect any server breach and file permissions on the server can limit potential damage.
- Imagine a wireless LAN where access controls are employed at the link layer (MAC validation, WEP encryption), network and transport layer (VPN tunneling, firewall access controls based on IP/port) and application layer (HTTP filtering and content inspection). A "war driver" would have to penetrate all these to accomplish the attack objectives.

Combined, these illustrate how powerful layered security can be. But, there's no single blueprint for designing security measures. Just as no two onions share the same number, density and thickness of layers, no universal blueprint for layered security will apply to every organization.

Ten Recommended Security Practices

To defend the integrity of your company's networked assets, we recommend following "best practices" and security measures as a foundation. The list below is our "Top 10" recommended security practices, although there certainly are other steps that can—and should—be taken.

1. Physical security. Think beyond the obvious measures usually taken to secure company offices. Do you reclaim identity cards and access tokens from employees when they are terminated? Do you provide anti-theft guidelines and equipment for mobile employees? Have you confirmed that wireless LAN antennae are appropriately placed and adjusted to reduce broadcast radio beyond your premises? Do you have a process defined to ferret out rogue WLAN access points (APs)? Have you swept your phone network to assure that no unauthorized modems are connected?

2. Secure perimeters. Internet firewalls meet the 90-percent rule: Properly configured, they block the noisy, low-level inbound attacks. But blocking inbound traffic is only part of the job. Limit outgoing access to only those external (public) services that users absolutely need, to reduce "cyber-slacking" and to defeat "back channels"—malicious trojans, root kits and spyware that may have wormed their way into your network. There's more at stake than simply being a good "netizen:" In our litigious society, you may be held liable if someone proves that your failure to meet accepted best security practices caused them quantifiable damages. Add layers to your perimeter security by placing firewalls close to servers. Restrict and encrypt traffic so that only authorized users can see and transfer sensitive data. Arm every teleworker and mobile computer with personal firewall and VPN software.

Require a user to supply something he knows, something he has and something he is

3. Authentication. It's high time to get rid of weak username/password authentication. Use two-factor authentication, based on tokens, digital certificates or biometrics, alone or in combination. Requiring a user to supply "something he knows, something he has and something he is," is effectively using layered credentials to harden authentication, creating a strong foundation for other measures that permit access by authenticated users while blocking all others.

4. Content inspection. Complement desktop antivirus measures with gateway software and firewall application proxies that can block malicious code. Worms inevitably will find desktops where virus definitions are not routinely updated. Apply and maintain a uniform content-blocking policy—for example, deny all ActiveX controls, unsolicited

Spam mail and potentially dangerous MIME types like .exe and .zip. Establishing the right filters can take time, but blocking malicious content on the way in is far more efficient than cleaning up numerous infected desktops.

5. System and server integrity. Many exploits allow attackers to gain administrative control of operating systems and access file systems. Third party, system-integrity software (sold by vendors like WatchGuard, Entercept, Immunix and Tripwire) adds a layer of access control beyond that already embedded in *NIX and Windows OSs.

6. Information integrity. Use file system encryption to protect stored data, especially on laptops and PDAs. If data is stolen but encrypted, it's useless to the thief. Think about integrity in your data archival process: Encrypt and digitally sign archived information. Remember to archive configuration information along with other sensitive data. Use VPN tunnels that provide per-packet confidentiality and data integrity checks. Think beyond remote access and site-to-site with VPNs; tunnels also can be used to protect intranet and inter-departmental email from eavesdropping by "insiders" or lurkers on wired and wireless LANs.

Effective security measures are a cost of business

7. Availability. Availability is a security metric—*denial of service* is a common and crippling attack. Identify mission-critical servers, security systems and network connections, and determine where you need high availability, redundancy, mirroring and diversity. These counter-measures allow you to better withstand DoS attacks and ensure business continuity.

8. Access Controls. Access controls enforce security and acceptable use policies. *Granularity is important.* Blanket access privileges, where everyone, from secretaries to CEOs, has the same access permissions, should be avoided. Limit access to applications and systems that each user absolutely needs, according to your prescribed security policy. Block everything else. Remember, the best baseline for security policy is to prohibit anything that is not expressly permitted.

9. Intrusion prevention, detection and rejection. While intrusion detection provides a valuable security service (see *BCR*, May 2002, pp. 42–45), consider building your networks to be immune to attacks.

Intrusion prevention involves the proactive monitoring of your network to assure that security measures are operating as intended, in-use software is kept current with patches and security updates, and that only approved services are operating. Recall that most attacks exploit known CVEs; keeping up with patches is far and away the most effective antidote.

10. Auditing and Logging. Log, log, log… then log some more. Logging and auditing are like blood tests, x-rays and MRIs. They tell you what's happening in your network. Over time, you will be able to distinguish what is normal from abnormal on your network. Log and audit file analysis can reveal trends and anomalies, and may help you avoid an incident or simply help you improve security measures. Early intervention or threat mitigation will be cheaper than post-incident cleanup and forensic analysis.

Conclusion

The security industry too often relies on fear, uncertainty and doubt (FUD) to sell products and services. The goal of this article is to inform, educate and, in so doing, ratchet what sometimes seems to be a depressingly dismal security baseline a little tighter. The proposition we hope you can sell within your organization is simple: If lax security practices can cost your organization considerable economic pain and suffering, can stringent security practices, over time, save you money?

While it's admittedly difficult to convince anyone that security is a revenue-generating investment, network security is no less a part of "the cost of doing business" than other preventative measures. Shop operators accept that they must pay for snow removal, for the simple reason that shoppers can't shop if they can't park. Networked businesses must pay for attack prevention. It's about access and availability. And availability is a security metric□

Companies Mentioned In This Article

CNN (www.cnn.com)

Computer Economics (www.computereconomics.com),

Computer Security Institute (www.gocsi.com)

eBay (www.ebay.com)

Entercept (www.entercept.com)

Immunix (www.immunix.org)

Information Systems Audit and Control Association (www.isaca.org)

Microsoft (www.microsoft.com)

Tripwire (www.tripwire.com)

WatchGuard (www.watchguard.com)

Yahoo (www.yahoo.com)