Before the Senate Governmental Affairs Committee
"Protecting Federal Systems from Cyber Attack"

Mar. 2, 2000

Testimony of Kenneth Watson
Cisco Systems Inc.
Manager, Critical Infrastructure Protection

Chairman Thompson, Ranking Member Lieberman, distinguished members of the Senate, I appreciate the opportunity to speak with you today about network security best practices.

Cisco Systems is serious about network security, and about its implications for the critical infrastructures on which this and other developed nations depend. Cisco predicted that the Internet would change the way we work, live, play and learn. Just four years ago this was considered a bold statement, but today few would argue that the Internet is changing every aspect of our lives. The Internet economy is creating a level playing field for companies, countries and individuals around the world. In the 21st century, the big will no longer outperform the small – rather, the fast will beat the slow.

The Internet was originally built to share information among scientists and other researchers in a trusted academic environment. No one considered the need for information security or that its commercialization would proceed as rapidly as it has. Over the last 10 or 15 years, we have gradually become dependent on networks, not only for conducting electronic business, but also for delivery of vital goods and services, like electricity, communications, water, oil and gas, as well as controlling transportation and financial transactions. Network security solutions are equally applicable to both the private sector and government networks. While network protocols, vulnerabilities, countermeasures, and best practices are common, regardless of business sector, function, or mission, no two companies or federal departments will have the same requirements or optimum solutions at any given time. And those requirements and solutions will change over time.

So how do you decide on a "best practices" solution? Many companies have their own solutions, and in fact, the Federal Chief Information Officers Council is conducting a study to investigate best practices for federal departments and agencies. I would like to offer a simple way to organize network security technologies and practices, and talk a little about what Cisco has seen in customer networks.

There are many ways to organize security technologies and activities--it's important to choose one and then carry it out. Here is ours--it's called the "Security Wheel."

Figure 1. The Security Wheel

Good security must be based on policy. One of our teams was out installing an intrusion detection system, and the company CEO wanted a list of the top ten web sites visited by his employees. He was also in the process of buying a second T-1 line because of his company's increasing demand for bandwidth. We showed him that the top seven or so weren't related to his company's business--in fact, they were to sports scores, porn sites, etc. He was furious, and wanted names. "Heads will roll!" We advised him that the list represented a majority of his company, and he would do better to establish a simple web use policy. He sent a memo to all employees, showing the "top ten" list, and stating that browsing the web with company computers for non-business-related use would be restricted to before and after business hours and during lunch. This told his employees two things: he could see what they were doing, and he cared. Almost instantly, his need for a second T-1 vanished.

After setting appropriate policies, a company or organization must methodically consider security as part of normal network operations. This could be as simple as configuring routers to not accept unauthorized addresses or services, or as complex as installing firewalls, intrusion detection systems, centralized authentication servers, and encrypted virtual private networks.

A basic tenet of military combat engineers is that an unobserved obstacle will eventually be breached. The same is true in networks. Hackers will eventually figure out a way through or around static defenses. The number and frequency of computer attacks is constantly on the rise -- there are no "vacation periods." As such, a critical part of the security wheel is to monitor one's network infrastructure and then respond to attempted (or successful) attacks.

The next stop on the wheel is testing a network. Organizations should scan their own networks regularly, updating electronic network maps, determining what hosts and services are running, and cataloging vulnerabilities. They should also bring in experts to conduct independent network security posture audits once or twice a year to provide a more thorough assessment of vulnerabilities and to get independent, outside recommendations regarding countermeasures, security patches, and other improvements.

Finally, there must be a feedback loop in every "best practice." System administrators must be empowered to make improvements. Senior management must be held accountable for network security, and those involved in the day-to-day operations must have their attention. Only by collecting and managing appropriate network security data, through audit logs, intrusion detection and response systems, and network scans, can management make intelligent decisions and improve the network's security.

If you were to ask me what the most important step is, I would give you two answers: one for the short term, and one for the long term. In the short term, the best thing any company or government entity can do is to conduct a security posture assessment along with a risk assessment, to establish a baseline security state. Without measuring where you are, you can't possibly figure out where to go or how to get there.

Last week's issue of *Information Week* includes a report from our security consulting team on vulnerabilities we have seen while conducting security posture assessments in customer networks. We grouped vulnerabilities into three categories: denial of service, reconnaissance, and access. Denial of service vulnerabilities allow an outsider to block normal network traffic to a server. Reconnaissance vulnerabilities permit an attacker to gather information that may prove useful to a future attack. Access vulnerabilities allow attackers to alter or manipulate data in a network. I've attached some suggestions to this testimony for identifying and remedying the most common vulnerabilities, which apply to any network, public or private.

For the long term, the best thing we can do together is to close the alarming skills gap. The requirement for highly skilled security specialists is increasing faster than all the training programs combined can produce qualified candidates. Universities are having difficulty attracting both professors and students. The government is also having a hard time retaining skilled security specialists. We in the private sector are building and maintaining state-of-the-art security training programs, and we're collaborating with education institutions and training partners to provide a wide base for delivery. We're also helping the Office of Personnel Management to identify knowledge, skills, and abilities, ongoing training requirements, and career management and mentoring ideas for a Federal IT security workforce. This human resources issue is by far the most critical information security problem we face, and the solution must be based on government, industry, and academic collaboration.

This committee recently proposed new legislation to strengthen federal network security, S. 1993. Two provisions of this bill closely parallel what we in industry have been saying for some time: security must be promoted as an integral component of each agency's business operations, and information technology security training is essential to the success of any network security improvement program. Each department and agency should execute its own programs based on tailored mission and risk analyses.

Corporate network perimeters are blurring. That's also true for the lines between government and industry. The Internet knows no boundaries, and we're all in this together. We are very enthusiastic about

the new Partnership for Critical Infrastructure Security, a voluntary organization of some 120 companies from across the country dedicated to improving the network security of our critical infrastructures. Already we have seen early fruits of this effort: 210 key executives attended a planning retreat here to begin to address interdependency vulnerabilities, information sharing, awareness and outreach, legislative and regulatory issues, research and development and workforce development. As we further build the relationship between the public and private sectors, we hope the great spirit of cooperation, led by the Department of Commerce and the Critical Infrastructure Assurance Office, will continue.

We will continue to work together to raise the bar of security overall, worldwide, so that we can empower our citizens and customers to take full advantage of the Internet economy in the Internet century.

I would be glad to take any questions.

Top Internet (External) and Intranet (Internal) Vulnerabilities and Recommended Fixes

This table outlines the vulnerabilities most often encountered by the Cisco Secure Consulting Services teams over the last six months. The vulnerabilities and their recommended fixes are applicable to any public or private Internet Protocol network.

Vulnerability

Fix

1. Internet

A. Denial of Service

Outdated, unnecessary network services (such as echo, chargen, systat, netstat)

Disable services as they are not typically required

Remote buffer overflow in the bootp network service

Disable bootp / disallow bootp access from the Internet. Bootp is a DHCP sub-service and there is no reason to run this service with access from the Internet

Remote buffer overflow in FTP network service

Update FTP server software to current release, apply security patches, enhance monitoring

B. Reconnaissance

Portmapper provides RPC sub-service information

Disallow access to the RPC portmapper from the Internet

SMTP network services verify and expand

Update SMTP server software to current release, apply security patches, enhance monitoring

NFS network service allows remote users to obtain info on exports

Restrict access to the NFS server from the Internet

Statd RPC network service

Disable the service; disallow access to the statd service from the Internet

Cold Fusion web servers

Use configuration control on the web server, apply vendor patches, remove sample pages, enhance monitoring

C. Access

Weak user authentication (default accounts, common accounts, joe accounts, null passwords)

Routine auditing of user selected passwords, password strength policy

SMTP mail relay

Update SMTP server software to current release, apply security patches, enhance monitoring.

Anonymous FTP access

Update FTP server software to current release, disable anonymous, apply security patches, enhance monitoring.

SMTP Pipe From

Update SMTP server software to current release, apply security patches, enhance monitoring.

SNMP Private community string

Change SNMP community names to something non-intuitive, disable access the SNMP from the Internet

Vulnerability

Fix

2. Intranet

A. Denial of Service

Outdated, unnecessary network services (such as echo, chargen, systat, netstat)

Disable services as they are not typically required.

FTP pasv

Update FTP server software to current release, apply security patches, enhance monitoring.

Remote buffer overflow in the bootp network service

Disable bootp if not required, apply vendor security patches, enhance monitoring

Remote buffer overflow in FTP network service.

Update FTP server software to current release, apply security patches, enhance monitoring

B. Reconnaissance

RPC Portmapper provides RPC sub-service information

Update RPC portmapper software, apply security patches, enhance monitoring

Finger provides username information

Disable the finger network service, apply vendor security patches, enhance monitoring

SMTP network services verify and expand

Update SMTP server software to current release, apply security patches, enhance monitoring.

Statd RPC network service

Disable the service, apply vendor security patches, enhance monitoring

SNMP public community string

Change SNMP community names to something non-intuitive, disable access the SNMP from the Internet

C. Access

Weak user authentication (default accounts, common accounts, joe accounts, null passwords)

Routine auditing of user selected passwords, password strength policy

SMTP mail relay

Update SMTP server software to current release, apply security patches, enhance monitoring

SMTP Pipe From

Update SMTP server software to current release, apply security patches, enhance monitoring

SMTP Pipe To

Update SMTP server software to current release, apply security patches, enhance monitoring

SNMP Private community string

Change SNMP community names to something non-intuitive, disable access the SNMP from the Internet