

**Hearing on Internet Security Issues
Senate Commerce Committee
Subcommittee on Telecommunications
March 8, 2000**

**Testimony of Mike Fuhrman
Manager, Cisco Secure Consulting Services Group
Cisco Systems Inc.**

Chairman Burns and distinguished senators, I am Mike Fuhrman of Cisco Systems. As you may know, Cisco is the world's largest manufacturer of equipment that connects people and businesses to the Internet. We are based in San Jose, California and have substantial operations in Massachusetts, North Carolina and Texas.

I manage our company's Secure Consulting Services Group, which helps ensure the security of some of the best-known sites on the Internet. My team of engineers and specialists evaluates the protective measures being employed by our customers and helps them respond to anyone or anything that threatens the integrity of their systems. As last month's hacker attacks on some of the world's busiest web sites graphically demonstrated, this is a task that requires constant vigilance.

Cisco's security specialists were among those who responded to the so-called "denial of service attacks" that temporarily blocked access to several web sites beginning Feb. 7. I'm happy to tell you that we were able to help some of our customers quickly identify the technology being used in these attacks, employ effective countermeasures and beat back repeat efforts by hackers to obstruct access.

In a nutshell, hackers initially were able to briefly shut customers out of some targeted web sites by bombarding those sites with more information – some of it false or misleading – than they were able to process. In a way, it was the Internet equivalent of trying to shop on the day after Thanksgiving, when the crowds are overwhelming. But in this case, the problem was nobody knew the rush was coming and therefore we weren't quite prepared to handle it.

After these assaults, there was some overheated speculation about whether the public can depend on the Internet as a reliable means of doing business and sharing information. The lesson to be learned from these attacks is *not* that hackers have some kind of technological edge that enabled them to do what they did. On the contrary, the technology employed in these attacks is well known to those of us in the systems security field and proper defenses against that technology are widely available.

The lesson is that events like these can be anticipated and managed with diligence and proper planning. The technology community showed that it can respond swiftly and effectively, taking steps to quickly mitigate the attacks and to make it harder for similar assaults to succeed in the future.

It's important to note that, in all of these assaults, service to targeted web sites was interrupted only for relatively brief periods. It's also important to note that while these attacks blocked access to some targeted computer systems, they do not appear to have penetrated the outer defenses of these systems. We know of no case in which hackers obtained access to confidential customer information, such as credit card numbers, or did lasting damage to any of the targeted sites.

And it's important to note that the technology community has already joined with the federal government to respond more effectively should attacks like these be repeated in the future. The community and the government are forming an organization that will disseminate critical information quickly and widely if the Internet is threatened.

We at Cisco Systems keenly understand the importance of this task. We will conduct \$12 billion worth of business over our own web site this year, and our employees are able to perform about 95 percent of their work on the site.

Cisco Secure Consulting Services recently conducted a six-month survey of 33 businesses connected to the Internet and measured their "state of security." We found that, on average, one out of every three devices connected to the Internet was vulnerable to some form of attack. But we also found that over 90% of the vulnerabilities could be solved with technology that is readily available, if the technology is properly employed and constantly updated.

This is easy to say and extraordinarily difficult to do. A decade ago, the Internet was little more than a clunky mechanism that a few educational and research institutions used to trade messages we now know as email. The blazing speed at which the Internet has developed – and the equally rapid pace at which threats to Internet security have evolved – make it hard even for those who build and operate web sites to keep pace.

But businesses and others who operate web sites are learning that security must become an ever-more-important concern. The number of companies who have come to Cisco for assistance in securing their networks has grown by over 50% during the last 12 months alone -- a very encouraging statistic. And we have all learned that one thing the technology community can do collectively to increase is to share information about up-to-the-minute developments in systems security.

The community has joined with the federal government to do just this. Even before last month's attacks, industry leaders had joined to form the Partnership for Critical Infrastructure

Security. The PCIS is a voluntary organization that is working to share information about threats to the Internet and other crucial networks, and determine how best to respond to those threats. About 120 companies are cooperating in this effort.

And last month at the White House information technology summit, Cisco was one of about 40 Internet companies that agreed to develop a structured mechanism to react to events like the recent hacker attacks. As with the PCIS, industry is coordinating its activities with the federal government.

We believe that this public-private partnership is the most effective response to these recent attacks. In the private sector, incentives must be put into place to encourage all web sites to deploy security technologies to protect themselves and their customers from hacker attacks.

In the public sector, we are grateful that the Federal Bureau of Investigation has devoted significant resources to investigating these attacks and we hope the perpetrators will be prosecuted to the fullest extent of the law. We encourage the federal government to serve as a model for private industry by equipping its own computer systems with the best security measures possible.

This, too, will not be easy. Both the government and private enterprise are having difficulty attracting and retaining enough skilled professionals in the field of systems security. I'm happy to tell you that the private sector has joined with the Office of Personnel Management to help the government in this area by developing training and mentoring programs. Again, we regard this as an excellent example of public-private partnership.

At this time, however, we do not ask Congress for new laws in the area of Internet security. Cooperation, not regulation or legislation, will insure that the Internet remains secure and at the same time open to the broadest possible public access.

The Internet is, and should always remain, an open medium. No one can insulate the Internet and everything connected to it from all threats or guarantee that no attack on any particular Internet site will succeed. Even our oldest, most established public infrastructures pause on occasion -- power and telephone lines come down, water mains break, highways become clogged -- and, like them, the Internet will occasionally have localized difficulties. These are but potholes on the information superhighway, which we will fill in as fast as they appear -- learning how to prevent similar potholes in the future.

These recent attacks actually demonstrated that the technology community can quickly identify threats to the Internet, quickly act to eliminate them and quickly take measures that will reduce the impact of similar threats in the future. This spirit of innovation and rapid development propels the Internet's exponential growth and ensures that the Internet will remain secure as it continues to grow.

Thank you. I look forward to your questions.