Internet Security

Submitted Testimony of Dave McCurdy
President
Electronic Industries Alliance

For the
Subcommittee on Science, Technology and Space for the Senate Commerce Committee
Monday, July 16, 2001

Chairman Wyden, Senator Allen, members of the Subcommittee on Science, Technology and Space, I appreciate the opportunity to submit testimony today on behalf of the Electronic Industries Alliance. I thank the Chairman for holding today's hearing on Internet security. There are few issues that are of more importance to the 2,300 member companies of EIA.

The Internet has become indispensable to the way we do business. The Internet empowers organizations to conduct e-commerce, provide better customer service, collaborate with partners, reduce communications costs, improve internal communication, and access information quickly.

In the rush to benefit from the Internet, organizations often overlook significant risks. For example, the engineering practices and technology used by many system providers do not produce systems that are immune to attack. Most network and system operators do not have the resources and technical expertise to defend attacks and minimize damage. Policy and law in cyberspace lag behind the pace of change. And lastly, security practices are underdeveloped, poorly disseminated and erratically followed.

For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated users can use them. Subsequently, serious attackers have a pool of technology they can use and mature to launch damaging attacks and to effectively disguise the source of their activities.

Attack technology is developing in an open source environment and is evolving rapidly. Technology experts and users are improving their ability to react to emerging problems, but we are behind. Significant damage to our systems and infrastructure can occur before effective defenses can be implemented. As long as our strategies are reactionary, this trend will worsen.

Our dependence on the Internet and the increased prevalence of attacks have created a true challenge for policymakers. As policymakers contemplate how to best protect the Internet and try to ascertain the proper role of government on the Internet, the reality remains: as a rule, technology has exponentially outpaced the establishment of sound policy.

As a result, it is incumbent upon the business community to take the lead in providing answers to Internet security. Similar to the Y2K crisis, only when our corporate boardrooms recognize their fiduciary responsibility to provide secure systems that Internet security will be addressed adequately.

Relatedly, the Electronics Industry Alliance recently formed the Internet Security Alliance (ISA) in conjunction with Carnegie Mellon University's CERT Coordination Center and a cross-sector of private companies including NASDAQ, Mellon Financial and AIG. The Alliance is an industry-led, global, cross-sector network focused on providing solutions to the challenges of the Internet economy. The mission of ISA is to bring Internet security to the forefront in corporate boardrooms worldwide.

Current Internet Security Policy

The control of U.S. cybercrime/cybersecurity policy has traditionally been viewed as an issue for the law enforcement and national defense communities -- not an economic policy issue. Solutions have been expressed in terms of criminal sanctions, counter-terrorism efforts and law enforcement training rather than the prevention managed by the users of the information assets, like businesses and individuals.

However, law enforcement and national security communities do not have all the answers. In addition to leadership from private industry, the following goals need to be met in any national policy:

- A National strategy from the President after consultation with leadership of constituencies for coordinated responses to threats and attacks, like those developed for Y2K including:
    - Establishment of empowered organizations for sharing information about cyber-threats, attacks and remedies such as the Internet Security Alliance, the sectoral ISACs, and similar government and international groups
- Incentives for industrial and government institutions to adopt top-down policies of institutional security – including information technology/network security – that include:
    - Clear designation of responsibility/delegation from CEO
    - Creation of risk management plan
    - Investments in employee enculturation and user education
    - Establishment of best practices regarding high value / high risk environments in information technology, for example:
        - Establishment of organizational CIO
        - Employee education on IT security practices
        - Deployment of best practices technologies
            - Firewalls
            - Antiviral software
            - PKI authentication/encryption for e-mail/Internet

- In government, necessary training and funding for these types of programs.

What we need to avoid in establishing a national policy:
New technology-specific criminal statutes that will result in the hobbling of vendor industries and slowing of deployment of leading edge technologies to the mass of internet users.

Where can the private sector help?

Organizations must search for an industry-led, global, cross-sector network focused on providing solutions to the challenges of the Internet Economy. We are at risk, and the business community must make it a leadership priority. The following are examples of what the private sector should be doing:

Information Sharing
Maintaining an adequate level of security in this dynamic environment is a challenge, especially with new vulnerabilities being discovered daily and attack technology evolving rapidly in an open-source environment. To help organizations stay current with vulnerabilities and emerging threats the private sector must concentrate on providing the following:

- **Vulnerability catalog*:*** a complete record of past vulnerability reports. New entries would be added to the catalog as they were reported.

- **Technical threat alerts*:*** in the form of "special communications" provide early warning of newly discovered security threats and are updated as analysis activities uncover additional information. Ranging from alerts on newly discovered packages of malicious code, such as viruses and trojan horses, to in-depth analysis reports of attack methods and tools, these reports would help organizations defend against new threats and associated attack technology.

- **Member information exchange*:*** augmenting the basic services listed above, an organization would have to develop an automated information sharing mechanism that allows business and individuals to anonymously report vulnerability, threat, and other security information that they are willing to share with other secure channels.

- **Threat analysis reports*:*** today the great majority of Internet security incidents are conducted by unknown perpetrators who act with unknown motivations to achieve unknown goals. Managing security risks in the long-term will require a better understanding of the perpetrators and the economic, political and social issues that drive them.

Best Practices/Standards
Effective management of information security risks requires that organizations adopt a wide range of security practices. From basic physical security controls that prevent unauthorized access to computing hardware, to user-focused practices on password selection, to highly-detailed system administration practices focused on configuration and vulnerability management, these practices help organizations reduce their vulnerability to attacks from both outsiders and insiders.

- **Practices catalog*:*** beginning with existing practice collections and standards, and in collaboration with any participating companies an organization must develop a catalog of practices that span the full range of activities that must be addressed when developing an effective risk management program. The catalog will contain high-level descriptions of the required practices and should be made publicly available

Security Tools
While a sizeable commercial marketplace has developed for hardware and software tools that can be used to enhance an organization's security and a variety of tools can now be purchased, comprehensive tool sets are lacking. To fill the gaps, organizations build their own or find and evaluate public domain tools – a time consuming and expensive activity. An organization would have to establish a tools exchange: a restricted access repository where network administrators only can exchange special purpose tools they have created as well as information about, and evaluation of, public domain tools available over the Internet.

Policy Development
While there are many things an organization can do to enhance its security, some issues require broad action. For example, overall security could be improved through increased information sharing between industry and government, but FOIA (*Freedom Of Information Act*) regulations deter companies from sharing sensitive information with the government. Other issues like privacy and the proposed HIPPA legislation could also affect network security. An organization needs to identify these overarching issues and work with the appropriate industry and government organizations to advocate policy that effectively addresses the issues.

Other Critical Areas

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Enhanced incident response capabilities – The incident response community has handled most incidents well, but is now being strained beyond its capacity. In the future, we can expect to see multiple broad-based attacks launched at the Internet

at the same time. With its limited resources, the response community will fragment, dividing its attention across the problems, thereby slowing progress on each incident.

- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.
- The problem is the fact that the demand for skilled system administrators far exceeds the supply.
- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.
- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer criminals is unlikely, and thus little deterrent value is realized.
- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. There is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.
- There is little evidence of improvement in the security features of most products. Developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. Until their customers demand products that are more secure, the situation is unlikely to change.
- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

Summary

While it is important to react to crisis situations when they occur, it is just as important to recognize that information assurance is a long-term problem. The Internet and other forms of communication systems will continue to grow and interconnect.

- More and more people and organizations will conduct business and become otherwise dependent on these networks.
- More of these organizations and individuals will lack the detailed technical knowledge and skill that is required to effectively protect systems today.
- More attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain.
- The network and computer technology will evolve and the attack technology will evolve along with it.
- Many information assurance solutions that work today will not work tomorrow.

Managing the risks that come from this expanded use and dependence on information technology requires an evolving strategy that stays abreast of changes in technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks. To move forward, we will need to make improvements to existing capabilities as well as fundamental changes to the way technology is developed, packaged, and used.

Attacks will happen – they will become more sophisticated as our technology becomes more sophisticated. The best defense we can take as a nation is to ensure our networks and systems are properly fortified against them.