Cyber-Security: Private-Sector Efforts Addressing Cyber Threats

Testimony of Dave McCurdy
President, Electronic Industries Alliance
Executive Director, Internet Security Alliance

Before the
Subcommittee on Commerce, Trade, and Consumer Protection
House Energy and Commerce Committee
2322 Rayburn House Office Building at 1PM
November 15, 2001

Chairman Stearns, Ranking Member Towns, and members of the Commerce, Trade and Consumer Protection Subcommittee: I appreciate the opportunity to testify today on behalf of the Internet Security Alliance. I am deeply thankful to Congressmen Stearns and Towns for holding this informative hearing on the private sector's efforts to address cyber threats.

Since September 11th, the business community has become more security conscious than ever before. There is real alarm among companies concerning not only physical security but also cyber security, and with good reason. According to the CERT/CC at Carnegie Mellon's Software Engineering Institute the number of attacks on the Internet has increased at an exponential rate. The CERT/CC handled over 20,000 incidents in 2000 and are now estimating that they will now handle over 40,000 incidents in 2001. Each one of those "incidents" could ultimately bloom into Code Red or Nimda attack within hours of its detection. The threat is critical. Corporations and the government find themselves on the front lines defending the critical functions of the national infrastructure, as well as the assets of American companies.

In addition, attacks are becoming more destructive, widespread and more difficult to contain. Consider the following information on costs of cyberattacks that businesses have faced recently.

The Costs of Cyberattacks

- SirCam: 2.3 million computers affected
  - –Clean-up: $460 million
  - –Lost productivity: $757 million
- Code Red: 1 million computers affected
  - –Clean-up: $1.1 billion
  - –Lost productivity: $1.5 billion
- Love Bug: 50 variants, 40 million computers affected
  - –$8.7 billion for clean-up and lost productivity
- Nimda
  - –Cost still be determined

In April of 2001, Carnegie Mellon University and the Electronics Industries Alliance formed the non-profit **Internet Security Alliance** to advance the efforts of the private sector in the information security debate. You may know that the majority of the Internet, over 80%, is owned and operated by the private sector. Private sector leadership is essential to determining an overall strategy to increase the strength and survivability of the Internet. The Internet Security Alliance seeks to help in this endeavor.

As the Internet continues to ingrain itself as a linchpin of American business and with concern growing that the cyber environment is ripe for attack, industry now more than ever needs an independent, non-partisan organization that offers comprehensive, universal threat sharing and assessment, and collaborative solution development. We need to create a new paradigm for global information sharing to help companies that rely on the Internet deal with the growing threats to their continued success and growth.

Furthermore, 80 percent of technical vulnerabilities are common to all organizations, and misperceptions about robust security can lead even the most attentive security engineers to expose their systems to attack. Industry needs to develop universally recognized information security practices capable of being pushed down through supply chains so evolving Internet threats can be effectively mitigated and deterred. You are only as secure as your weakest link.

The Internet Security Alliance is one of the few organizations working on behalf of industry to address these issues. With its international and multi-industry segment member representation and access to a network of more that 40,000 loyal systems administrators and security engineers who diligently report new threats and vulnerabilities, the Internet Security Alliance is redefining the concept of information sharing. On a near real-time, systematic basis, the alliance provides companies large and small with access to trusted and reliable information, solutions and decision support tools to help mitigate the vulnerabilities and emerging threats we are here to discuss today.

Driven by some of the brightest security minds in industry and academia, the alliance has also begun work on a robust set of best practices that will serve as guiding principles for companies and their supply chains as they evolve their security policies and procedures. Our efforts enable companies to allocate their limited resources on other projects, such as deploying intrusion detection systems, firewalls, and raising security awareness within own organization.

Using the collective experience the Internet Security Alliance and its members, we can effectively promote sound information security practices, policies and technologies that enhance the security of the Internet and global information systems.

Why is the private sector involvement so important?

The Internet Security Alliance applauds the efforts of the current Administration in its dedication to raising the awareness of cyber-threats and cyber-terrorism. Its leadership on the recent cyber-attacks such as Code Red and Nimda were invaluable to testing the true value of both private and public partnerships. On the government side, however, officials tend to view private sector participation and the agency involvement in terms of sectors or "stovepipes" (see attached chart for the government organization chart for cyber-security), therefore creating barriers to true information sharing. The private sector is critical of this approach and is looking for more inclusive participation from all sectors. In order effectively address cyber-threats, collaboration and communication should be cross-sector and horizontal to all companies and government entities (where appropriate). We all face a common threat with respect to cyber-terrorism and vulnerabilities and need to work together in order to protect our most critical assets.

International problem vs. U.S. centric problem: Cyber-Security

The Internet knows no boundaries and is accessible from most parts of the world. As the Internet continues to be a tool that promotes the openness of ours and many other societies, it brings along vast risks and vulnerabilities. The Internet operates with no bias or cultural differences…it provides information and interaction. Since the concept of the Internet was based on the issue of trust, we can see the probability of its being compromised fairly easily.

With that in mind, we would be foolhardy to not communicate with other nations on their experiences and potential remedies for cyber-attacks that have happened on their networks. Not taking into account the expertise of foreign security experts would put the U.S. effort at a severe disadvantage. In addition, if the U.S. is not inclusive of other countries in this global problem, we stand to weaken our resolve to protecting ourselves by operating with limited knowledge of potential threats.

Proactive Measures vs. Reactive Response

Finding solutions to cyber-security vulnerabilities and attacks has been historically reactive. Attacks happen, analyses made and a patch provided, if possible. We cannot continue to solve individual attacks on a case-by-case basis, and not address the larger problem. A better approach is to implement practices and policies that improve the protection of our networks by thwarting a higher percentage of attacks. In other words…becoming more <u>proactive</u> in our approach to cyber-security. By promoting practices currently in place for more security-focused companies and tailoring them for other sectors, additional protection could be provided. Many companies, especially medium-sized and smaller firms are vulnerable and looking for assistance in determining what security practices can help them better protect their systems.

Private and Public Partnerships

The security and survivability of the Internet depends on the cooperation between the private and public sectors. Congress should promote interaction between government and the private sector and should also address issues such as exemption from FOIA and anti-trust barriers. In addition, Congress can set a great example for the private sector by increasing the security of all government systems, which historically have been out-dated and have not met minimal standards for security.

The Internet Security Alliance is able to act as a bridge between the private sector and public sector by promoting best practices and appropriate data sharing mechanisms. The Internet Security Alliance is also involved in the following activities:

- Providing thought leadership on information security issues
- Representing industry's interest on information security issues before legislators and regulators
- Creating mechanisms that cause rapid development and implementation of information security practices, policies and technologies
- Identifying and standardizing best practices in Internet security and network survivability
- Creating a collaborative environment to develop and implement information security solutions
- Promoting universal sharing of information and intelligence on emerging threats/vulnerabilities/ countermeasures

• **Information Sharing**
– Providing vulnerability catalog, threat alerts and analysis, executive communications, call center, trend briefings, economic impact analysis
– Shaping and influence practices and resources at CERT/CC to meet the needs of industry

• **Best Practices/Standards**
– Establishing common benchmarks
– Evaluating relevance of existing standards, define gaps and agree on relevant and uniform criteria for standards moving forward
– Developing a Software Seal of Approval

• **Policy Development**
– Providing decisive influence on the public policy issues whether nationally or internationally
– Targeting cybercrime and terrorism, privacy, information sharing, corporate responsibility and leadership on information security issues

• **Security Tools**
–Sector-tailored versions of OCTAVE®
–Sharing of R&D expertise of Alliance members

To summarize, only by combining the strengths of both the private sector and public sector on issues such as early warning detection and information dispersal, promotion of best practices, agreement over sound information security policies will we be able to turn the tide on the cyber-security threat facing our nation.

The Internet Security Alliance is poised to represent and promote the needs and views of the private sector on cyber-security. We thank the committee for its interest and for allowing us to participate in this necessary and timely hearing.