TESTIMONY OF JOHN W. THOMPSON
Symantec Corporation
before the
HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
Hearing on "Computer Viruses: The Disease, the Detection, and the Prescription for Protection"
November 6, 2003

Chairman Upton, Ranking Member Markey, members of the Subcommittee, thank you for the opportunity to provide testimony today on computer Viruses. This is a timely and important topic and on behalf of Symantec, I appreciate your willingness to examine the issue and challenges surrounding it.

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of client, gateway and server security solutions for virus protection, firewalls and virtual private networks, vulnerability management, intrusion detection, Internet content and e-mail filtering, remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries.

We are at an important juncture with regard to cyber security. The threats we are seeing today are more sophisticated, more aggressive and are able to spread more rapidly than ever before. Equally important, the time from the discovery of a new vulnerability to the release of an exploit targeting that vulnerability is rapidly shrinking. I make the analogy of an exploit being an "unlocked door" of a building and an exploit being a break-in by someone who knows about the unlocked door. These two phenomena have made the Internet increasingly vulnerable to attack.

We are already beginning to see the early stages of what are called flash threats, threats that are near instant in their delivery. These are threats in which human reaction time is probably not fast enough. A good example would be the recent Slammer worm, which, at it's a peak rate, infected 90 percent of the vulnerable systems in just 15 minutes. This speed of propagation, combined with the reduction of the time to exploitation, raises serious issues about the approach our nation is taking to protect our networks.

We have taken the initial steps to improve our cyber security, from the largest corporations or infrastructures to the individual end user, but security is an evolving process and we must continue to be aggressive in our corporate IT security governance and in educating the individual user about good cyber security practices.

Congress passed the Federal Information Security Management Act (FISMA) to improve the protection of government systems. This risk-based management approach provides a guideline for Agencies to improve the protection of their critical assets.

In the private sector, associations like the Business Software Alliance and TechNet are working on information security governance projects to assist the private sector on improving the protection of their infrastructure. I am pleased that Symantec is a part of both of those projects.

I would also point to the upcoming Department of Homeland Security Summit scheduled for December. The summit's intent is to bring together government and industry leaders to work on implementing the National Strategy to Secure Cyberspace. This is a positive sign of the commitment to work together on this important issue.

But more needs to be done. If anything, the recent attacks during the month of August served as a "wake-up" to all of us. In fact, the threat of major cyber attacks causing significant damage to our infrastructure is real and still exists today.

Let me give some additional insight into the nature of the threats we are seeing with information from our recently released Internet Security Threat Report, a comprehensive semi-annual view of cyber security activity. The report covers information on vulnerability discoveries, malicious code trends and network-based attacks. I have included a copy of the report for submission with this testimony.

The report represents the distillation of data from over 500 Symantec managed security customers and over 20,000 registered sensors monitoring worldwide network activity in more than 180 countries. We would argue that it provides the most complete view of the health of the Internet available anywhere today.

As I mentioned earlier, the time from vulnerability discovery to exploit is rapidly shrinking. For example, the SQL Slammer worm attack from January of this year, exploited a vulnerability discovered about six months earlier. Just a

few months later that benchmark changed significantly with the release of the Blaster worm. This blended threat exploited a vulnerability just 26 days after disclosure.

We have also seen that 64 percent of all new attacks targeted vulnerabilities less than one year old. Moreover, of all the new attacks documented in the first half of this year, 66 percent targeted what would be classified as highly severe vulnerabilities. Symantec documented over 1400 new vulnerabilities, a 12 percent increase from last year. In looking at the severity of these new vulnerabilities, we saw a 6 percent increase in those carrying a 'high' severity rating and a 21 percent increase in those of 'moderate' severity. These trends should be a major concern to all of us. As they continue, we will need new security paradigms to appropriately protect our cyber-infrastructure

Early warning and alerting capabilities, strong patch management, and solid internal processes to respond when a new vulnerability is discovered, may be the difference between protecting critical systems and having them compromised.

With regard to malicious code trends, we observed a much more aggressive attack pattern. The Blaster worm, as an example, infected systems at an average rate of 2,500 computers per hour.

We are also starting to see the use of viruses and worms to attack newer applications, such as instant messaging and peer to peer networking.

In fact, of the top 50 malicious code submissions we received in our laboratory during the first half of this year, 19 used peer-to-peer and/or instant messaging applications --- an increase of almost 400 percent in just one year.

So, the trends suggest that the overall rate of attack activity rose 19 percent. Companies experienced, on average, 38 attacks per week compared to 32 for same period last year.

By highlighting some of these key findings, we see the importance of prioritizing cyber security at work and at home.

I would like to focus on two key areas I believe are important to improving cyber security of our IT infrastructure: Corporate IT security governance and user awareness.

Corporate IT security cannot continue to be an afterthought or add-on approach. It should be integrated into the overall management plan for an organization. In today's connected world, we rely heavily on our IT infrastructure to conduct business, and it should not be compromised due to a lack of security measures. The resource constraints that many organizations are facing, coupled with the increasing rate of attacks, make this a daunting challenge. In many instances, these attacks are dealt with in a reactive rather than a proactive manner, making the task even more difficult.

In developing a cyber security plan, we believe it should focus on the following areas: ensuring overall business continuity, adhering to regulatory compliance, enabling organizations for their "e" initiatives, and, establishment of a security policy and implementation plan. All of this must be done with a watchful eye on balancing risk and managing cost to ensure both system availability and security.

In discussions with enterprise organizations, they cite three main drivers of the need to look at security in a more holistic manner. They include the disappearing perimeter, the increase in threats and the lack of security expertise.

The question really is "how do we adequately address these issues?" I believe IT security requires a new level of governance at the senior level. It requires a top down approach that reaches across the organization's departments and functions. It requires the creation of a culture of security.

IT governance must be a part of the overall governance of an organization. Doing so will ensure that IT is aligned with the organization to deliver value to its constituents, that IT resources are responsibly utilized and that IT risks are mitigated and managed appropriately. Taking this a step further, information security should also fit in this broader view. For example, information security reports should go to senior executives in an organization and information security audits should be part of the overall audit program.

Furthermore, implementing security with real-time risk management is a key to preparation and protection. Organizations need to know where they are vulnerable, establish benchmark security levels and policies that will ensure compliance.

Let me now turn to education and awareness. We have often heard the statement that we, as individual users of the Internet, have an obligation to protect our piece of cyber space." I firmly believe this is true.

A vulnerable system, regardless of whether it is a home user surfing the web on a broadband connection, a wireless mobile computer at Starbucks, or a telecommuter working from home, all can open the door to threats.

As we continue to see increased computing power for the individual user and continued adoption of high-speed connections, we must focus on providing a safe and secure environment for that user, which includes using a firewall and a regularly updated anti-virus program.

I would point out that we often think of the individual user as only the home user, a view that is short sighted. As mobile computing becomes more pervasive we need to be aware at the enterprise of the potential holes to the network that could open up from customers, business partners or employees.

The perimeter to the enterprise is disappearing and steps must be taken to protect those critical assets not just at the gateway, but at all the end-points or access points being used in today's environment.

This means more than just implementing technology solutions. It means educating the employees through a well-organized security-training program. Employees need to be armed with the knowledge to responsibly protect our networks.

Symantec has taken an active role in promoting a broad-based awareness campaign through our participation as a founding member of the National Cyber Security Alliance.

In partnership with the Department of Homeland Security and the Ad Council, the Alliance recently announced a $1.8 million national cybersecurity awareness campaign. Symantec is a major supporter of this effort along with other leaders from industry and government.

The Alliance program will be designed to educate the home and small business users on the importance of using anti-virus and firewall technology, as well as tips to defend against online fraud. Further information from the Alliance can be found at www.staysafeonline.info.

A recent study by the National Cyber Security Alliance confirms the need for this broad-based campaign. That study showed that about 67 percent of high speed Internet users do not use firewalls and more than 60 percent do not regularly update their anti-virus software.

In addition to the National Cyber Security Alliance, Symantec has also created a tool that home users and small businesses can use. This tool, called Symantec Security Check, can be found at http://www.symantec.com/securitycheck , It is free service that scans an individual's system for vulnerabilities. To date we have conducted over 50 million scans. Of the 3.9 million people who were scanned and agreed to submit their data, 24 percent did not have any anti-virus protection, and 9 percent of those that did have some type of anti-virus solution did not regularly update their definitions. In addition, of the 1.35 million users who agreed to submit their data to our virus detection scan, 35 percent were infected with viruses or worms.

We need to broadly get the message out about the dangers and threats to our Internet infrastructure. The work by the National Cyber Security Alliance is a great example of the type of public-private partnership that is essential to promoting a safe and secure computing environment, and ultimately better protecting our critical infrastructure.

Let me close by saying that education and awareness of the individual whether in the largest multi-national corporation, small business or the home user is critical. Security is more than just installing a piece of software, it is using best practices, updating your anti-virus and practicing safe and secure computing to ensure that systems are safe and the nation's infrastructure is more secure.

Thank you.