Statement of John Schwarz
President, Symantec Corporation
House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Hearing on Worms, Viruses and Securing Our Nation's Computers"
September 10, 2003

Chairman Putnam, Ranking Member Clay, Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject: Protecting our nation's computers and our nation's critical infrastructure. A critical infrastructure that is heavily reliant on IT, and one that remains vulnerable to cyber attack.

Today, much of our economy and our critical assets are in digital form. We are a society that is becoming more and more dependent on Information Technology, yet we do not take the steps to protect those cyber assets to the same degree as we have our physical assets.

The cyber world is maturing and is pervasive in organizations as well as at home. It is also becoming more complex and vulnerable. The attacks are faster, less predictable, and more severe. The number of opportunities for exploitation also continues to grow at a rapid pace. In fact, it is estimated that on average, 70 new software or firmware vulnerabilities are discovered each week.

Last year, the number of new vulnerabilites reported was 81.5% higher than the previous year, and that number continues to rise today. We are also seeing an increase in the number of high and moderate severity vulnerabilities. They were reported as 84% higher than in 2001. These vulnerabilities are being exploited faster and more aggressively than ever. On average, we are identifying 450 new viruses each month, with many reaching high severity levels. Perhaps more alarming is the fact that once discovered, the time to exploit a vulnerability is rapidly shrinking. For example, the SQL Slammer worm in January 2003, utilized a vulnerability that was disclosed six months previously in July 2002. The recent Blaster worm utilized a vulnerability that was disclosed in July 2003 – just one month before exploit.

In the past, patch deployment was not as much of an immediate concern. Since fewer vulnerabilities were discovered, patching was less of a drain on resources. If an IT professional had to apply one new patch a quarter versus one a week, less resources, planning and potential down time was required. Additionally, it took longer for a worm or virus to propagate or spread and infect large numbers of systems, so response was much different.

In 2001, this all began to change. We saw the transition to "blended threats" with worms like Code Red, and Nimda containing multiple attack vectors. These blended threats, combine the attributes of a traditional worm and a hack attack, and are the biggest threat we face today.

This acceleration of threats, their severity and the speed of their infection, is evident in the Slammer, Bugbear, and most recently Blaster, and Sobig worms. The ability to respond to these blended threats has become more difficult. A few years ago Symantec's security response team had as much as two days to provide a solution to our customers, today that time has diminished to a matter of minutes.

By leveraging the vast number of new vulnerabilities, the potential introduction of entirely new, and more destructive forms of malicious code and cyber attacks tools represents a substantial future risk.

Looking forward the next generation of attacks, known as "Flash" threats have the potential to infect massive portions of corporate networks and even the entire Internet within minutes or even seconds The recent Blaster or SQL Slammer worms are hints of these types of threats. According to available research data, SQL Slammer infected 90% of the initially vulnerable systems in approximately 10 minutes. Such threats require entirely new proactive systems to stop them as no entirely reactive infrastructure will ever be fast enough to protect against threats spreading at these speeds.

Let me now discuss some actions that we believe can improve our cyber security.

1. Awareness and Education

Educating our consumers, our small businesses, the operators of the critical infrastructure and all levels of government on the importance of protecting our systems is essential. We need a broad awareness campaign that reaches out to all users of the Internet. The growing use of always-on broadband connections by home users and small businesses represents a significant amount of computing power, which left unprotected can be taken over and used as zombie machines to damage our networks and the hinder the commerce and services that flow through them. At the least, these home users should deploy a minimum protection of firewall and anti-virus technology. The remote or wireless-connected worker is also becoming more prevalent and can unknowingly open up a corporate network to potential vulnerabilities and attack through unprotected connections.

Enterprises and government agencies should engage their employees in security awareness programs to ensure better protection of their systems. Whether it's reminding them not to post their passwords on a yellow sticky pad on their computer, or enacting corporate best practices to change those passwords on a regular basis making them difficult to break.

At the enterprise and organizational level, the issue of IT security has for too long been an administrator or a CIO issue. This needs to change. Cyber security needs the attention of the CEO and the boardroom. Only then can we institute the necessary cultural change and focus enough attention and resources to truly address this issue.

2. Cyber crime

We saw the arrest of Jeffrey Lee Parson for writing a variant of the Blaster worm, but we have yet to find the bigger culprits, the original writer or writers of the recent flurry of worms. We need to realize that protecting the Internet is really a global issue; one that requires better international cooperation. First, we need better resources for law enforcement to work on computer forensics, and we need cooperation from industry to assist prosecutors in building cases. Second, we require better harmony in cyber crime laws, the Council of Europe's cyber crime treaty is a good starting point. Third, industry should reach across borders when appropriate, to share information on best practices, threats and vulnerabilities, in order to gain a measure of early warning of potential attacks. The Industry Information Sharing and Analysis Centers or (ISACs) can be that vehicle. Finally there should be a single point of contact in government so that those leaders can communicate at a peer level in times of major cyber attack.

3. Research and Development

Today, industry and government tends to look at the more immediate threats to our cyber infrastructure, rather than a holistic view of encompassing threats of today and tomorrow. It is a view that needs to change. As mentioned earlier, flash threats may be on us in the near future and we must be more proactive in our cyber security practices focusing on behavior blocking and better patch management, including the use of fast, safe and non-disruptive patching. Given the shrinking time from discovery to exploit, we should engage in projects like real-time vulnerability scanning, management and patching and we must do it together in partnership; industry government and academia alike.

4. Audit and Risk Analysis

Security is not a static issue and thus requires regular assessments of systems and vigilance on the part of IT mangers, and for that matter all users of the Internet. I commend the Committee for it efforts to enact programs like GISRA and FISMA, which require annual risk assessments of government systems and also require actions to improve the protection of those systems. The Committee's oversight in this area is invaluable. This is not just something that the government should do, and I would encourage enterprises, large and small to follow this example of regular security assessments.

In closing, let me issue this challenge to industry, government and the individual users: We must take cyber security more seriously and we must do it together.

The increasing prevalence of blended threats and the potential for even more fast-spreading and damaging exploits is a serious threat to our nation's information infrastructure and the economic benefits that we derive from it. We need strong leadership from industry and government to promote awareness and education on cyber security, more resources for law enforcement to investigate and prosecute cyber criminals, strong research and development partnerships to tackle the challenges of future

threats to the Internet, and more vigilance from business and governments by putting resources and support behind a proactive IT security program.

But most importantly we all as individual users of the Internet, need to do our part, to protect cyber space. Experience shows that effective implementations of security solutions cost in the range of 6-8% of overall IT budgets. Few corporations outside of the finance sector, or government departments, have allocated such levels of funding to this critical need. It is time that we put our resources to work to minimize the risk of a serious disruption of our national cyber infrastructure.

Thank you and I look forward to your questions.