Testimony of Don Frischmann

Senior Vice President, Communications and Brand Management,
Symantec Corporation
Sponsor, National Cyber Security Alliance (NCSA)

Before the
House Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"*Locking Your Cyber Front Door - The Challenges Facing Home Users and Small Businesses.***"**

June 16, 2004

Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay, members of the Subcommittee, thank you for inviting me to testify today on the important topic of cyber security for consumers and small business. My name is Don Frischmann, and I am the Senior Vice President for Communications and Brand Management at Symantec Corporation. I am also here representing Symantec as a sponsor of the National Cyber Security Alliance, a nonprofit organization whose mission is to educate home users, children, young adults and small business owners on the importance of cyber security best practices. I am honored to be here today, and I look forward to joining my distinguished colleagues from government and industry to discuss this important topic Today I would like to address some of the challenges that consumers and small businesses face, as well as offer some recommendations on how we can overcome these challenges.

Challenges:

We are at an important cyber security crossroads. On one hand American Internet usage has grown to more than 144 million active users according to Nielson ratings. Today, the Internet is being used to do everything from monitoring baby's sleeping to banking, to commanding the combination refrigerator/oven to start cooking dinner before we leave the office. As our society and economy becomes more dependent on Internet connectivity, unfortunately Internet threats are growing just as fast.

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 shrinking rapidly. I make the analogy of the vulnerability being an "unlocked door" of a home and the 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 beginning to see the early stages of what are called flash threats, threats that are near instantaneous in their dissemination. These are threats in which human reaction time is probably not fast enough. A good example is the Slammer worm, which, at its

peak rate, infected 90 percent of the vulnerable systems around the world in just 15 minutes.[Adam: Please confirm that we have data in support of this statistic.] 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. More information about these trends can be found in our semi-annual Internet Security Threat Report, available on the Symantec website. I would also like to submit a copy of the report for the record.

Some of the specific challenges that consumers and small businesses face include: eliminating viruses, blocking hackers, safeguarding personal information, fighting spam, increasing online productivity, recovering lost or damaged files and safely removing confidential data that small businesses no longer need.

Consumers are storing more valuable, private information on their computers – from personal financial information, digital photos and confidential data and documents brought home from the office for evening or weekend work. Additionally, they are using the Internet to conduct e-commerce on a regular basis. Consumers' increasing reliance on their computers and the Internet allows people to be more efficient and innovative. However, the reliance also makes protecting sensitive data and mitigating Internet threats important issues. Internet threats that affect consumers include viruses, worms, Trojan horses, blended threats, privacy invasions, hackers, spam, cyber predators and inappropriate Web content. Threats such as spam are a hot button among consumers as they not only pose an annoyance, but they also usher-in the possibility of individuals falling prey to online fraud through phishing emails, which are messages that appear to come from trusted sources, but are instead used to scam individuals into disclosing personal information, including credit card numbers, and social security numbers.

According to a March 2004 survey conducted by Symantec and Applied Research, one in three users between the ages of 18-64 has clicked on a spam link. In the case of senior citizens, only 23 percent of such have clicked on a spam link, but 47 percent of those senior citizens who responded did not employ a spam fighting solution. Children also fall

prey to Internet threats, including spam. A June 2003 survey conducted by Symantec and Applied Research found that more than 80 percent of children surveyed who use email receive inappropriate spam on a daily basis.

Small Business Challenges

The challenge for many small businesses is that they lack the resources to employ a full-time IT manager. Computer related issues are often handled by the small business owner or the most technologically knowledgeable employee. Many times, the person responsible for computer issues does not have sufficient understanding of Internet security threats or knowledge of how to protect the small business against malicious code, hackers and privacy invasions.

Spam continues to be a hot issue among small businesses due to its annoyance and its negative impact on productivity. A December 2003 survey conducted by Symantec and InsightExpress found that 64 percent of small business owners who responded to the survey reported an increase in spam over the past six months, with 33 percent noting dramatic increases. Symantec's small business spam survey found that 42 percent of small business owners responding would consider abandoning email for business correspondence if the spam situation worsens.

Small businesses have been exposed and will continue to be exposed to Internet threats such as malicious code and unwanted intrusions. According to Access Markets International (AMI) Partners, Inc., small businesses do see the need to protect their critical assets. Thus, AMI expects that total spending on security solutions among small businesses is expected to grow 25 - 30 percent annually in developed countries worldwide (April 1, 2004).

Recommendations:

In light of these trends, the consumer and small business segment is a critical component for improving safe and secure computing and one that would benefit from continued awareness and education initiatives. The President's National Strategy to Secure

Cyberspace acknowledges that awareness is a key component to ensuring our overall cyber security.

Everyone who relies on the Internet has an interest in promoting its security. Users, whether at home or at work, need to know the simple things that they can do to help block intrusions, cyber attacks, or other security threats. Security is an evolving process and we must continue to be aggressive, especially in educating the individual user about good cyber security practices. Implementing cyber security best practices enables users to be less reactive when a cyber attack occurs, and become more proactive in the protection of personal data and property, promoting the country's economic stability, and ultimately our national security. A recent study by the National Cyber Security Alliance confirms the need for this broad-based education. That study showed that nearly 67 percent of high speed Internet users do not use firewalls and more than 60 percent do not regularly update their anti-virus software to protect against new threats.

When it comes to Internet security, the first challenge with consumers and small business users is to get past the "it can't happen to me" mentality. The second challenge is to help them understand how these online threats can affect them and the simple steps they need to take to protect their computers and their value data. These steps include a combination of technology tools and best practice processes.

The National Cyber Security Alliance is developing a three-year national cyber security awareness campaign beginning this fall. This awareness campaign targeted at home users and small businesses, will use various vehicles to raise awareness of the cyber-security issue and provide actionable steps people can take to protect themselves. In conjunction with the "StaySafe Online" awareness efforts, the campaign will include dissemination of cyber security tips, which are already available through the NCSA's main website: www.staysafeonline.info. On this site, visitors can also find self-tests, tool-kits for each audience, helpful links and more. One of the NCSA's top ten tips is to remind computer users to keep their anti-virus and other security software up-to-date by regularly downloading anti-virus definitions, intrusion signatures, and vulnerability patches.

As a provider of products and services to consumers, Symantec has found that home users also want easy-to-use integrated solutions to protect their computers against Internet threats. These bundled packages are easy to install, user-friendly, and protect against malicious code, hackers, privacy infringements, spam and inappropriate web content. We believe it is essential to make it easy for non-technical customers to use technology that will protect them and the systems they rely upon.

Small business owners, are beginning to realize the need to move beyond just anti-virus solutions to integrated security solutions that include intrusion detection, VPN, firewall, remote network security management and spam control. To address this need, security companies such as Symantec are offering appliances that provide affordable, high performance, all-in-one technology for small businesses. These appliances are easy to install and requires minimal maintenance.

Some small businesses have just a couple of computers, and their IT infrastructures more closely resemble a consumer profile than that of an enterprise. Regardless of size, though, small businesses need to protect the critical data from Internet threats. For small offices that employ ten or fewer people, an integrated security suite can protect small businesses from online threats by eliminating viruses, blocking hackers, safeguarding personal information, fighting spam, increasing online productivity, recovering lost or damaged files and thoroughly deleting confidential data that small businesses no longer need.

There are also many small businesses that have a more sophisticated IT infrastructure that includes desktops, network servers and remote computers. These businesses need multi-layered security at every tier, offering one easy-to-manage solution that includes firewall protection, intrusion detection and interacts seamlessly with anti-virus software to keep systems safeguarded against viruses, worms, Trojan horses, blended threats, and other technology used for malicious activity.

In recent years, the public's attention to cyber security issues has risen dramatically, particularly as more and more Internet users transition to broadband connections. No longer is it unusual for us to hear about viruses and worms on the morning news. Most users (though not all) know it is critical to have anti-virus software. Some users (but certainly not all) also understand the importance of personal firewalls. As I pointed out at the beginning of my remarks, we are at a cyber security crossroads, and we still have a long way to go to raise the level of cyber security awareness with the general public. But, I do believe that we are taking the initial steps and that we can succeed in better securing our infrastructure.

Thank you for the opportunity to speak to you today. I would be happy to take any questions.