

Testimony of Douglas Sabo

**Member, Board of Directors, National Cyber Security Alliance
Director, Government & Community Relations, McAfee Security**

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

**“Protecting Our Nation’s Cyber Space:
Educational Awareness for the Cyber Citizen”**

April 21, 2004

Chairman Putnam, Vice Chairwoman Miller, Ranking Member Clay, members of the Subcommittee, I want to thank you for inviting me to testify today on the important topic of cyber security educational awareness initiatives. My name is Douglas Sabo, and I am a Member of the Board of Directors of the National Cyber Security Alliance (NCSA) as well as the Director of Government and Community Relations for McAfee Security, a provider of cyber security and intrusion prevention solutions based in Santa Clara, California. I am honored to be invited to be here today on behalf of the NCSA, and I look forward to joining my distinguished colleagues from government and industry alike to discuss with this Subcommittee the challenges of awareness and education in cyber security. Today's hearing on the cyber secure citizen is a timely and important topic, and on behalf of the National Cyber Security Alliance, I appreciate your willingness to examine the issue and highlight its importance.

The National Cyber Security Alliance is a unique partnership among the Federal government, leading private sector companies, trade associations and educational organizations. Through the NCSA's Web site, www.staysafeonline.info, this partnership aims to educate Americans about the need for computer security and encourage all computer users to protect their home and small business systems. In its efforts, the NCSA has worked particularly closely with the National Cyber Security Division of the US Department of Homeland Security. Assistant Secretary for Infrastructure Protection Robert Liscouski and National Cyber Security Division Director Amit Yoran both have been extremely supportive of the NCSA's efforts.

Before I talk about the NCSA's initiatives, it is important to underscore why this issue of the cyber secure citizen is important.

Trends in Cyber Security: Why Education and Awareness are Important

In order to understand the increasing importance of education and awareness and the role of the consumer and small business, allow me to discuss two particular trends in cyber security:

1. Threats are Changing

The cyber security threat is changing. No longer are we in a world where cyber exploits take months to gain momentum around the globe. Today, the "exploit window" (or, the time from the discovery of a new vulnerability to the release of an attack exploiting that vulnerability) is rapidly shrinking. At the same time, these exploits or attacks are becoming more sophisticated, more aggressive and more prolific at a faster speed than ever before.

In recent attacks, the time taken for a threat to be created to exploit a vulnerability has been about three weeks. This is the time between when the vulnerability exploited by Lovsan/Blaster, for example, was announced and when Lovsan/Blaster itself was discovered. This timeframe is significantly down from the six months that elapsed before CodeRed took advantage of the vulnerability in Microsoft IIS. In parallel, the exploits themselves, once unleashed, are much more prolific and harmful. The Code Red and Nimda denial of service worms spread around the globe in a day or less. In January 2003, the Slammer worm infected over 5,000 servers around the world in under three minutes, and infected 90 percent of vulnerable systems worldwide in just 15 minutes.

2. Growing (False) Sense of Security

As these threats are changing, there is a concern that a growing false sense of security among many Internet users has emerged. In some ways, perhaps we have become victims of our own success.

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 or while gathered around the office water cooler. Most users (though not all) know it is critical to have anti-virus software. Many users (but certainly not all) also understand the importance of personal firewalls. But how do their practices compare to their understanding?

The National Cyber Security Alliance, in conjunction with AOL, has conducted a number of surveys on these questions. In a June 2003 study, 86 percent of users felt their computer was very or somewhat protected from online threats, with 76 percent having anti-virus software and 59 percent having personal firewall protection. Obviously, that leaves 24 percent without anti-virus software and 41 percent without firewall protection. But we must look more closely at those who do have those protections. According to our study, 62 percent of those with anti-virus software do not regularly update it, and 67 percent of those with firewall protection do not have properly and securely configured firewalls. While the number of those with anti-virus and firewall protection has risen dramatically, a majority of those with these protections is not practicing secure behaviors. There is a disconnect between beliefs and practice, and we fear a false sense of security is the result.

In light of these trends, the consumer and small business audience is a critical component, and one that would benefit from continued awareness and education initiatives. Of course, we aren't the only ones talking about this. The President's *National Strategy to Secure Cyberspace* itself acknowledges that awareness is a key component to ensuring our overall cyber security:

Everyone who relies on part of cyberspace is encouraged to help secure the part of cyberspace that they can influence or control. To do that, users need to know the simple things that they can do to help to prevent intrusions, cyber attacks, or other security breaches. All users of cyberspace have some responsibility, not just for their own security, but also for the overall security and health of cyberspace. (*National Strategy to Secure Cyberspace*, pg 37, February 2003)

Our Response: National Cyber Security Alliance Initiatives

In response to these challenges, a coalition of companies, trade associations, organizations and government bodies came together to form the National Cyber Security Alliance (NCSA). The organizations sponsoring NCSA are diverse and bring a variety of expertise to the group. Industry representatives include: AOL, BellSouth, Cisco Systems, McAfee Security, Microsoft, RSA Security and Symantec. Trade associations include: Business Software Alliance, Cyber Security Industry Alliance, Information Technology Association of America, Internet Security Alliance and US Chamber of Commerce. Non-profit organizations include: CyberSmart!, EDUCAUSE, InfraGard and the Information Systems Security Association. Finally, government agencies include: US Department of Homeland Security (National Cyber Security Division), US Federal Trade Commission, Federal Bureau of Investigation and National Institute of Standards and Technology. We are actively looking for additional companies, organizations and government agencies to become sponsors of the NCSA.

This group of agencies, companies and organizations understands the important role that consumers, small businesses and our youth play in contributing to our overall cyber security. With that role in mind, the NCSA has created and developed a number of education and awareness initiatives addressing cyber security:

Initiative: National Cyber Security Awareness Campaign

First, as a cornerstone of our effort, the NCSA is developing what we hope (resource permitting) will be a three-year national cyber security awareness campaign. This campaign, targeted at home users and small businesses, will use various vehicles to raise awareness of the cyber security issue and steps people can take to protect themselves. Whether through radio, print or television, these public service announcements will talk about the important role all consumers play in ensuring the security of our information infrastructures. In developing this campaign, the NCSA is working closely with the US Department of Homeland Security, one of our major sponsors. A campaign of this size and scope does require significant resources. The NCSA has begun an effort to raise these resources.

In conjunction with these awareness efforts, the campaign also will include dissemination of cyber security tips. This effort, referred to as "Stay Safe Online," already has begun through the NCSA's main website: www.staysafeonline.info. On this site, visitors can find self-tests, top security tips, helpful links and more. For our latest list of *Top Ten Cyber Security Tips*, please see Appendix A of this testimony.

Initiative: Tips and Toolkits

Our second major project involves developing toolkits for small businesses and specific subgroups within the home user audience. These toolkits will include materials, guidebooks and training programs for each group based on the NCSA's *Top Ten Cyber Security Tips*, including a version of the top ten tips for children (K-12). We are in discussion with a variety of other organizations, including the Small Business Administration, InfraGard, ISSA, NIST, FBI and the Internet security provider (ISP) community, to establish key partnerships so that the cyber security tips, toolkits and training programs can be disseminated as quickly and as far as possible to each targeted audience.

Initiative: Youth Education

Our third major effort will focus on educating our youth on cyber security practices to make sure the next generation of users is cyber secure. Through partnering with outside organizations such as CyberSmart!, we hope to develop and disseminate cyber security curriculum to educators across the country. The NCSA also supported a national poster contest in which students were asked to creatively depict the importance of cyber security.

In addition to these initiatives, the sponsors of the NCSA are actively developing other creative efforts as well. We look forward to sharing these with the Subcommittee in the future.

National Awareness Campaigns: A Glance

As we have stated, the NCSA expects our national cyber security awareness campaign to be a cornerstone of our effort to reach consumers and small businesses. In crafting this campaign, we have turned to many other examples of similar efforts, through which government and others came together to develop an educational effort to reach individuals, raise awareness and change behavior. We share a few leading examples here, gathered from the website of the Ad Council (<http://www.adcouncil.org/campaigns>), for informational purposes:

Issue: Homeland Security

Sponsor: US Dept of Homeland Security; Alfred P. Sloan Foundation

Goal: To educate Americans on how to respond to future terrorism-related emergencies

Campaign: Ready.gov

Issue: Healthy Lifestyles

Sponsor: US Dept of Health and Human Services

Goal: To lower the percentage of Americans who are overweight or obese due to sedentary lifestyles and unhealthy diet and exercise habits

Campaign: Healthy Lifestyles and Disease Prevention Campaign

Issue: Wildfire Prevention

Sponsor: USDA Forest Service, National Association of State Foresters

Goal: To remind Americans of the importance of outdoor fire safety and wildfire prevention

Campaign: Only You Can Prevent Wildfires

Issue: Drunk Driving Prevention

Sponsor: US Dept of Transportation/NHTSA

Goal: To reduce alcohol-related vehicular injuries and deaths

Campaign: Friends Don't Let Friends Drive Drunk

Issue: Crime Prevention

Sponsor: National Crime Prevention Council; US Department of Justice

Goal: To reduce crime and build safer communities by encouraging teens and adults to engage in their communities

Campaign: Invest in Youth for a Safer Future

Issue: Promote Voting

Sponsor: Federal Voting Assistance Program

Goal: To encourage 18-24 year olds to participate in upcoming elections

Campaign: Decision Guy

NCSA's Invitation

On behalf of the NCSA, I would like to formally invite you, Mr. Chairman, the Members of this Subcommittee and your Congressional colleagues to learn more about the National Cyber Security Alliance:

- 1) We invite Members to place a link and the NCSA logo on your website so that your constituents can be made aware of the information that is available to them in this area.
- 2) We invite Members to use our monthly cyber security tip newsletter (in development) to send out to their state and local publications.
- 3) We invite Members to turn to us to assist in educating their constituencies of the threats online and how to protect themselves. The NCSA has brochures and other materials that Members can use in town hall meetings. We are happy to assist your staff with coordinating these programs and will work to provide you a representative from the NCSA for your local events.
- 4) We invite you to look at our awareness campaign plans as well as other efforts that have had national exposure and impact.

Summary

Mr. Chairman, the challenge before us today is significant. Cyber attacks are accelerating and becoming more dangerous. Reported vulnerabilities are on the rise and are being exploited more frequently and faster. Consumers and small businesses are using the Internet at higher and higher rates. While many have basic security technologies in place, most are not following the practices needed for them to be effective.

There are steps we can take to make a real difference. As the NCSA, we have come together to develop real initiatives in awareness and education. We do not believe we have all the solutions. In fact, we embrace the philosophy, "let a thousand flowers bloom." But we do hope that our initiatives can contribute to the overall progress in educating consumers and small businesses to protect themselves—and in turn, all of us.

As is often said, security is a journey, not a destination. We applaud your Subcommittee and Congress for continuing to put energy into addressing the cyber security challenge. In return, we pledge to you the NCSA's support to continue to work with government, industry and academia to develop initiatives to address these specific challenges.

I thank you again for the opportunity to testify here today, and I look forward to answering any questions the Subcommittee may have.

Appendix A: NCSA's Cyber Security Tips

NCSA's Top Ten Cyber Security Tips for Home Users and Small Business

(from www.staysafeonline.info)

1. Use "anti-virus software" and keep it up to date.
2. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.
3. Protect your computer from Internet intruders -- use "firewalls".
4. Regularly download security updates and "patches" for operating systems and other software.
5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.
6. Back up your computer data on disks or CDs.
7. Don't share access to your computers with strangers. Learn about file sharing risks.
8. Disconnect from the Internet when not in use.
9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.
10. Make sure your family members and/or your employees know what to do if your computer becomes infected.

1. Use "anti-virus software" and keep it up to date.

Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

2. Don't open email or attachments from unknown sources. Be suspicious of any unexpected email attachments even if it appears to be from someone you know.

A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. If you are determined to open a file from an unknown source, save it first and run your virus checker on that file, but also understand that there is still a risk. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line (e.g. "Iloveyou" or "Anna Kounikova") or if it otherwise seems suspicious (e.g., it was sent in the middle of the night). Also be careful if you receive many copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete! If you receive an email from a trusted vendor or organization, be careful of phishing, a high-tech scam used to deceive consumers into providing personal data, including credit card numbers, etc. For information about "phishing" go to the FTC document titled "How Not to Get Hooked By a

Phishing Scam”, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.pdf>. The best way to make sure you’re dealing with a merchant you trust, and not a fraudster, is to initiate the contact yourself. Type the merchant’s address into your Internet browser instead of clicking on a link in an e-mail.

3. Protect your computer from Internet intruders – use “firewalls”.

Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can’t gain access to your computer while you’re connected to the Internet. You can find firewall hardware and software at most computer stores and in some operating systems. Don’t let intruders in!

4. Regularly download security updates and “patches” for operating systems and other software.

Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes bugs are discovered in a program that may allow a criminal hacker to attack your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors’ web sites regularly for new security patches or use the automated patching features that some companies offer. Ensure that you are getting patches from the correct patch update site. Many systems have been compromised this past year by installing patches obtained from bogus update sites or emails that appear to be from a vendor that provides links to those bogus sites. If you don’t have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

5. Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.

Passwords will only keep outsiders out if they are difficult to guess! Don’t share your password, and don’t use the same password in more than one place. If someone should happen to guess one of your passwords, you don’t want them to be able to use it in other places. The golden rules of passwords are: (1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters, symbols and numbers, e.g., xk2&LP97. (2) Change passwords regularly, at least every 90 days. (3) Do not give out your password to anyone! For enhanced security, use some form of two-factor authentication. Two-factor authentication is a way to gain access by combining something you know (PIN) with something you have (token or smart card).

6. Back up your computer data.

Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Many people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

7. Don’t share access to your computers with strangers. Learn about file sharing risks.

Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to “share files”. This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don’t pay

close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

8. Disconnect from the Internet when not in use.

Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. and help protect others: disconnect!

9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.

The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year – do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

10. Make sure your family members and/or your employees know what to do if your computer becomes infected.

It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!