

Statement of Philip Reitinger

Senior Security Strategist, Microsoft Corporation

**Testimony Before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
House Committee on Government Reform
U.S. House of Representatives**

**Hearing on “Locking Your Cyber Front Door – The
Challenges Facing Home Users and Small Businesses”**

June 16, 2004

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee:

My name is Philip Reiting, and I am a Senior Security Strategist for Microsoft. Thank you for the opportunity to appear today. I would like to discuss the ways in which Microsoft is working with its customers and its partners to help make computing more secure for both small businesses and individual consumers. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High Tech Crime. For some time I have been concerned with criminal threats, and with the challenges posed in preventing, detecting, deterring, and responding to cyber crime.

At Microsoft, security is a top priority. There are fundamental challenges that we and the industry as a whole must address in order to enhance security for small businesses and individual consumers. First, software – regardless of vendor and development model – is highly complex and will always have vulnerabilities. Second, while we see increasing security awareness among our customers, some small businesses and many individuals do not understand the threat or how to defend against it. As a result, many do not enable firewalls, run anti-virus software, or regularly update their systems. Our response to these challenges is rigorous and extensive: We are working with our customers and partners to enhance software security and to make it easier to use security technology, to reach more small businesses and individuals, and, recognizing that security is a process and not a destination, to innovate and work with government to protect public safety.

I. Enhancing Security: A Top Priority

We launched our Trustworthy Computing initiative in January 2002. Within Microsoft, this initiative fuels technological innovation and yields security tools that help our customers enhance the security of their computers.

Many of our technological innovations were discussed in my colleague Scott Culp's testimony before this Subcommittee on June 2, 2004. In brief, we are building more secure software through the following four-part strategy:

- Streamlining updating processes and enhancing updating tools to make it easier for consumers and small businesses to install security updates;
- Pursuing "Engineering Excellence" to reduce vulnerabilities by using state-of-the-art engineering practices, standards, and processes throughout the entire software development cycle;
- Increasing isolation and resiliency so that systems are protected against entire vectors of attack even in the absence of necessary updates; and
- Improving authentication and access controls that govern who gets access to networks and computers, and how they establish access privileges.

We are producing new and useful tools for our small business and individual customers, giving them flexible but simple systems to obtain and install updates. We have introduced a feature called "Automatic Update" for our recent operating systems. This tool presents a user with options ranging from automatic downloads of updates and

scheduled installation to declining all updates. Similarly, on Microsoft.com we provide Windows Update, a web-based service which can identify missing patches for the Windows operating system and install them automatically if the user elects to do so. Later this year we plan to introduce Microsoft Update, which will provide the same service, but will also include other major Microsoft software as well as Windows.

At the same time, we improved the updating process by:

- Standardizing the operation of our security updates and installation technologies;
- Releasing updates once a month on a consistent schedule, to enable small businesses to plan update installations systematically and efficiently; and
- Reducing the update size where possible to make obtaining updates less burdensome.

One of the significant steps in the Trustworthy Computing initiative will take place later this year with our release of Service Pack 2 for Windows XP (“XP SP2”) which will include significant security upgrades – many of which are aimed directly at home and small-business customers. First, the Windows Firewall will be made easier to use, enhanced and turned on by default to help stop attacks even if a system is not updated. Second, XP SP2 will have a “Security Center” which will centralize security management and recommend guidance when action needs to be taken. Third, file attachment handling will be improved for email and instant messaging programs to help prevent the spread of attachment-based viruses. XP SP2 will also reduce the threat posed

by malicious code on web sites by enhancing customers' ability to prevent this code from running on their PCs.

Finally, and especially for customers with dial-up connections to the Internet, we have made available the Windows Security Update CD which we ship on request to customers free of charge. This CD includes Microsoft critical updates released through October 2003 and information on how customers can help protect their PCs. This CD is available for Windows XP, Windows Me, Windows 2000, Windows 98, and Windows 98 Second Edition.

II. Reaching Customers

While we pursue our Trustworthy Computing initiative, we also continue to reach out to customers directly and through partnerships with our industry peers and government.

Last fall we launched our "Protect Your PC" campaign (www.microsoft.com/protect) through a broad print and online campaign to encourage customers to take three essential steps to safeguard their systems:

1. Use a properly configured Internet firewall;
2. Regularly install security updates in their computers; and
3. Run up-to-date anti-virus software.

We also reach our customers on cyber-security issues in other ways. For instance, we will soon complete a series of security summits that have reached a broad array of

customers, including one summit that occurred here in Washington, D.C. on April 8, 2004. Further, we provide security web sites for small businesses (www.microsoft.com/smallbusiness/gtm/securityguidance/hub.msp) and individuals (www.microsoft.com/security/home and <http://security.msn.com>). These web sites provide our customers with basic knowledge on how to maintain an appropriate level of security and to avoid common internet-based frauds, such as “phishing” scams.

We have many partnerships to increase security awareness among small businesses and individuals. We are a member of the National Cyber Security Alliance, a partnership between the federal government and industry members with the goal of educating Americans on the need for computer security. The Alliance’s web site, www.staysafeonline.info, is a clearinghouse of security-related information designed to encourage small business and home users to protect their systems. In order to make this information even more accessible and understandable to consumers, we are partnering with the Alliance to produce an Internet security and safety booklet that will soon be made available to policymakers and others for distribution to citizens. In addition, we participate in the information technology industry’s Information Sharing and Analysis Center, the IT-ISAC, which issues bulletins on significant cyber security events. We also work with US-CERT to share information. And we helped found the Global Infrastructure Alliance for Internet Safety, a collection of global ISPs with the goal of helping to educate and protect consumers against the threat of malicious code attacks as well as emerging Internet threats.

III. Security as an Ongoing Challenge: Innovating and Working with Government

Secure computing is a process and a journey, not a final destination that can be reached. Threat models change over time, and we must change and innovate with them. Just as burglars find ways to defeat home security systems, cyber-criminals find new ways to attack computer systems. As a result, our industry must innovate continually while working with our customers to improve the security of their systems. These are difficult challenges, and they will be with us as long as we have connected computers and criminal attackers.

The government has an important role as well. It must increase the security of its computer systems and provide law enforcement officials with the tools, resources, and training they need to deter and investigate criminal attacks. Our government's hard-working officials – including those within the Departments of Justice, Homeland Security, and Defense, as well as state and local investigators – are often short-staffed, under-funded, under-trained, and lack state-of-the-art technology used by cyber criminals. Also, cyber attacks are an international problem requiring cross-jurisdictional cooperation – to that end, we urge the Senate to ratify the Council of Europe Cybercrime Convention to help streamline international criminal investigations.

Finally, we are constantly searching for new and better ways for industry and law enforcement to partner to protect public safety in this dynamic environment. One example is our Anti-Virus rewards program, which offers rewards for information leading to the arrest and conviction of cyber criminals in certain cases. This program recently encouraged individuals with information on the author of the Sasser worm to

step forward, leading to an arrest of the alleged hacker. We also assist and support the National Cyber Forensics Training Alliance (“NCFTA”), a joint government-industry organization, on investigations, online fraud, and online safety. In fact, to help protect the public from computer crime, Microsoft has placed an analyst on site at NCFTA who performs trend analysis and evaluates and forwards complaints received from users of Microsoft software and services. Microsoft is also in the process of donating software to the NCFTA to support its on-going mission.

Conclusion

Through our Trustworthy Computing initiative, we continue to develop innovative technologies and tools that enhance the security of our software, and to communicate with our customers about the importance of updating and securing their systems. We are working with our partners in industry and government to help consumers and small businesses enjoy safe, efficient, and productive on-line experiences.

I thank you for the opportunity to address the committee, commend your work on this issue, and look forward to your questions.