

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. MCHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LA TOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS K. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
Wm. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

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

**Wednesday, June 16, 2004
2:30 p.m.**

Room 2154 Rayburn House Office Building

Opening Statement of Chairman Adam Putman (R-FI)

I want to welcome you all today to this oversight hearing on "Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses."

In the past few years, the growth in access and use of the Internet, the increase in “always on” high-speed connections, and the rapid development and deployment of new computing devices has resulted in an expanding global computing network. Although these advances have improved the quality of life, this global network is susceptible to viruses and worms that can circle the world in a matter of minutes. The potential for more sophisticated and malicious cyber attacks is growing at an alarming rate. While businesses, educational institutions, and home users enjoy the benefits of using the Internet, these groups are not always adequately informed about the potential dangers of computer systems left vulnerable and unprotected.

This hearing is a continuation of a series of oversight hearings that the Subcommittee has conducted during the 108th Congress on the issue of cyber security. On April 21, the Subcommittee held a hearing specifically on educational awareness for all cyber citizens. Most recently on June 2, the Subcommittee conducted an oversight hearing on the cyber security and vulnerability management issues facing primarily large enterprises. The purpose of this hearing is to specifically focus attention on the challenges facing home users and small businesses. Today, the Subcommittee will examine the difficulties that these users confront in protecting their computers; actions taken by the federal government to create partnerships that will assist home users and small businesses

in their efforts to protect themselves against a variety of potential cyber threats; the role of software and hardware manufacturers in responding to the expectations and demands of the user community to provide the marketplace with higher quality and more secure products; the role of internet service provider's in helping to educate and protect their subscribers; and the tools and strategies available to home users and small businesses to lessen their exposure to risks.

Home users and small businesses are in a uniquely vulnerable position because their computers often face the same worms, viruses and automated attacks that business and government computers face. Yet, these users may not have the same level of resources available to mitigate these risks. Accordingly, it is critically important that all stakeholders examine tools and strategies to more comprehensively address this growing challenge.

Right now, home and small business users face many types of risk. Viruses and worms can disable home users' systems. Home users may also be tricked into downloading spyware. These programs can be harmless, yet extremely annoying, such as delivering a continuous stream of pop-up ads. Or they may be malicious, extracting information such as passwords and personal information for criminal purposes. Home users also face the threat of fraud and identity theft schemes, including a newer approach known as "phishing."

Small businesses face these same threats as well, but their challenges are compounded by the fact that they may have a network of machines to manage, as well as the additional challenge of employees using laptops and remote access. Of even greater concern, small businesses face the threat of disgruntled insiders who were once trusted users. Finally, small businesses may also have private information from their customers in databases that are connected to the Internet. Cyber criminals who gain access to this information may attempt to extort money out of small businesses to keep the breach quiet. The loss of reputation from such an incident could be devastating to a small business.

There are existing and emerging protections against these threats. Home users and small businesses can arm themselves with virus protection software to help stop any potential impact of worms and viruses. Use of firewalls can also help prevent some forms of spyware and attempts at unauthorized access to a user's machine. Automated patches are also a step in the right direction to help users stay up to date with protections against the most recently published vulnerabilities.

However, employment of these well-known protections is still inconsistent. Awareness of the available protections needs to be elevated so that basic computer security hygiene becomes a common practice amongst all users.

Increasing cyber security awareness will help users to protect themselves, but user awareness is only part of the problem. Many of the security problems that users face are rooted in products that were designed to deliver functionality, often without enough regard to security. We can no longer simply blame the users for their failure to mitigate vulnerabilities. The users are not responsible for the flaws and defects in the products that are the source of the vulnerabilities in the first place. I will continue to examine the progress being achieved by the manufacturers of software and hardware products in responding to the consumer and public demand for higher quality and more secure

products for the marketplace. I am encouraged by what I see as signs that the manufacturers are taking this demand seriously.

Vendors are starting to release products that are “secure by default” by enabling secure technical control settings and by requiring affirmative action by the user to enable features that could make the product less secure. Software and hardware vendors are making more significant commitments to their quality assurance programs in an effort to identify “bugs” and flaws prior to deployment of new systems. Collaboration among vendors to offer a bundled “suite” of security products to users, along with a more concerted effort to configure systems in a more secure manner “out of the box” will produce a more secure computing environment.

In addition to the efforts of the vendors to improve security of their products, the federal government needs to help improve the security of computer products and services through research and development. Inadequate tools exist in the marketplace today to conduct effective code evaluation in advance of deployment in an effort to identify flaws, defects, and even the potential of malicious code willfully inserted in a software product. By collaborating with partners in the world of academia and the private sector, the federal government should be working to support the development of such tools and other quality assurance tools that can make a meaningful difference in improving the quality and security of new IT products. The federal government has an important role in targeting R & D efforts to address such critical issues.

As a member of Congress, a home computer user, and a champion of small business, this problem hits close to home for me, and I plan to continue my efforts to improve cyber security in every sector of our nation. In furtherance of this effort, I convened a group of 25 leaders from business organizations, as well as representatives from academic and institutional communities, to form the Corporate Information Security Working Group (CISWG). The intent was to produce a set of recommendations that could form the basis of an action plan for improving cyber security for businesses and enterprises of all sizes and sectors. The group divided into subgroups, one of which was the Awareness, Education, and Training Subgroup. This subgroup’s mission was to identify, partner with and build on the good work of organizations that have or are developing campaigns that raise awareness on the importance of cyber security. The Awareness, Education, and Training Subgroup reported recommendations for three categories of users – small businesses, large enterprises, and home users.

For small businesses, the group suggested creating and distributing a small business guidebook for cyber security that explains cyber security risks in terms that are readily understood and that motivate small business owners to take action. I understand that efforts are under way to make this recommendation a reality.

For home users, the group suggested targeted efforts aimed at the mass market would help to educate these users. The group is seeking to build upon existing relationships and to forge new partnerships between organizations, corporations, and the government that will help educate the home user base on cyber security hygiene. I will continue my support for these initiatives and plan to reconvene the Corporate Information Security Working Group at the end of this month to further develop a number of the recommendations that were produced in Phase I.

On a related note, I would like to announce that I have taken an important step in furtherance of a recommendation from the CISWG. Yesterday, along with Chairman Tom Davis, I introduced H.R. 4570 to amend the 1996 Clinger-Cohen Act to place a greater emphasis on computer security within the Federal government. H.R. 4570 brings Clinger-Cohen in line with the realities of today's IT world by requiring agencies to specifically consider security when conducting systems planning and IT acquisition. I am confident that once H.R. 4570 is signed into law that it will help to strengthen the Federal government's overall efforts to improve the information security profile of its systems.

In closing, I want to make clear that securing the nation's cyber space is an urgent challenge, and we all have a role to play. The threat is real...the vulnerabilities are extensive...and the time for action is NOW! Unfortunately, there are no simple solutions. I will continue to examine the role that the Congress and the federal government can and should play in being a "partner in progress" in elevating the attention to this matter for all stakeholders. Education and awareness is a key element to advise all users about the tools and strategies to reduce the risks associated with a very real cyber threat.

I look forward to the testimony from today's witnesses and I thank you for your contribution to the security of our nation.