

**Testimony of Andrew Howell
Vice President, Homeland Security
U.S. Chamber of Commerce**

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

April 21, 2004

Chairman Putnam, Vice Chair Miller and Congressman Clay, my name is Andrew Howell, and I am Vice President of Homeland Security for the U.S. Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation representing more than three million businesses and organizations of every size, sector and region.

Thank you for giving me this opportunity to discuss the Chamber's cyber security awareness efforts. Also, Mr. Chairman, I would like to thank you for your leadership on this issue, and for recognizing the importance of enhancing awareness of cyber security among the public and private sectors.

The National Strategy to Secure Cyberspace, released in February of 2003, called for a "comprehensive, national awareness program to empower all Americans—businesses, the general workforce and the general population—to secure their own parts of cyberspace" (Page 37). The strategy asserts that everyone who uses the Internet has a responsibility to secure the portion of cyberspace that they control.

The Chamber supports this view. It is the responsibility of a person using a product to know how to use that product safely. However, we do not believe that raising awareness is the only solution to enhancing cyber security. Instead, it is one part of

the solution. Enhancing cyber security requires the combined efforts of users, technologists, and senior executives—those that use software and hardware, those that make software and hardware, and those who manage enterprises that rely on software and hardware to make the company operate. While technologists have a responsibility to make secure products, end users have a responsibility to use those products securely.

A good analogy to this is the automobile. While cars provide individuals with great benefits, they also can be dangerous. Therefore, cars come equipped with seatbelts. However, ultimately, it is the driver's responsibility to buckle his seatbelt and know how to operate the vehicle safely. The vehicle must be maintained with regular maintenance, and when there is a recall notice, the owner has a responsibility to take the car in for repair. At the same time, in the interest of selling more products, automakers continue to design cars with more safety features, and market those features to the consumer.

By promoting user awareness, we are not, as some maintain, blaming users for cyber vulnerabilities. Instead, it is through awareness that we highlight the issue of cyber security, inform people what they can do to manage risks, and, in the process, create a market of consumers who can intelligently factor security into their purchasing decisions. By informing users about what they can do to enhance their cyber security, we will reduce the number of breaches, reduce economic loss, and create a market that encourages the production of more secure products.

Moving the market to demand more secure products is an important component of enhancing our nation's level of cyber security preparedness. Ultimately, the market is better able to respond to security challenges than regulations will ever be. Whereas

market forces propel companies to be flexible, innovative and customer oriented, regulations are reactive and constrictive. As consumers of all types become more aware of information security risks and protective steps they can take, they will demand more secure products. Companies that recognize this market shift and sell products that exploit it will have an advantage over their competitors. The market remains a powerful vehicle for increasing cyber security, but before this power is fully realized, we need to better inform consumers on why cyber security is an issue that matters to them.

For these reasons, the U.S. Chamber of Commerce is committed to increasing the awareness of cyber security in the business community and explaining cyber security in terms that businesses understand. For too long, the issue of cyber security has been talked about in technological terms. As a result, many corporate leaders and small business owners view it as a technology issue that should be solved by technologists. From our perspective, this is a mistaken perception that must be corrected.

Recognizing this, in February of 2002, before the release of *The National Strategy*, we helped to create, organize and support the National Cyber Security Alliance (NCSA), a public-private coalition dedicated to raising cyber security awareness among small business owners and home users. Doug Sabo, of McAfee Security is an NCSA Board Member and will provide you with more details about the Alliance and its work.

At the same time, the U.S. Chamber of Commerce has regularly used our membership publications, including *USChamber.com*, to provide tips and guidance to small business owners, to explain why cyber security is important to their business and to offer easy

to implement advice on how to better secure their networks. Attached is the most recent version of this publication, which includes some tips for small business owners.

In December of 2003, the Chamber partnered with the Information Technology Association of America, the Business Software Alliance, TechNet and the Department of Homeland Security to host the National Cyber Security Summit. As part of the Summit process, an Awareness and Outreach Task Force was created to provide recommendations on implementing the awareness component of *The National Strategy*. The Chamber volunteered to serve as Secretariat for that Task Force, which is chaired by Dan Caprio of the Federal Trade Commission, Ty Sagalow of AIG, and Howard Schmidt of e-Bay.

Early in the process, the Task Force decided that it wanted to change user behavior and, as much as possible, provide incentives that will encourage people to do so. We targeted five key markets: small businesses, large enterprises, home users, state and local governments and K-12 schools and institutions of higher education. On March 18, 2004 the Task Force released its first report, detailing its completed work and next steps.

Soon after the summit in December, as part of Chairman Putnam's Corporate Information Security Working Group (CISWG) process, the Chamber was asked, along with NFIB, to co-chair the sub group on awareness. The work of the CISWG sub group focused on three audiences: small businesses, large enterprises, and home users. Mr. Chairman, as you well know, on March 3, 2004 we presented our report to you, detailing some recommendations our group thought were good next steps for these target markets.

Both our National Cyber Security Summit Task Force report and our report to the CISWG are attached to this testimony. I ask that that they be included in the hearing record.

To quickly summarize our findings, let me just touch on some highlights. For the small business audience, it was evident that before small business owners would upgrade or enhance their cyber security, they needed to understand their level of cyber risk. A company called nuServe, whose CEO, Kai Tamara Hare, Chaired the National Cyber Security Summit Small Business Working Group, agreed to make available, on a complimentary basis, the company's Cyber RiskProfiler. This interactive online tool allows small business firms to better understand their information security risks.

Also, it was clear to the Task Force, after some extensive research, that there is no practical guidance for small businesses seeking to better manage the risks they face online. To fill this void, the Task Force asked the Internet Security Alliance to produce a *Common Sense Guide to Cyber Security for Small Businesses*. As part of the process, Larry Clinton and his colleagues hosted 10 focus groups with 100 small business owners to better understand the needs of this particular market. Larry will discuss the Guide in more detail, but let me just say that initial feedback is very positive.

Finally, as an incentive to follow this Guide and use the RiskProfiler, AIG eBusiness Risk Solutions has agreed to provide cyber insurance credits, where legally permitted. All a company must do is demonstrate they use the RiskProfiler and follow the recommendations of the Guide.

For large enterprises, we proposed that the Department of Homeland Security partner with industry on a series of regional homeland security forums to discuss the role of the private sector in homeland security in general, and cyber security specifically. We envision this being a partnership between DHS, our task force and corporate C-Suite executives.

For home users, we noted our support for a national public service campaign to increase the level of cyber security awareness. Also, our participants contributed to the National Cyber Security Alliance's recently released "Top 10" tips for home users and small businesses.

All of the aforementioned recommendations were made by the National Cyber Security Summit Awareness and Outreach Taskforce and the CISWG Education and Awareness group. Yet let me also tell you about two additional markets covered by the National Cyber Security Summit Awareness and Outreach Task Force. One focused on K-12 Schools and Institutions of Higher Education, and the other on State and Local Government.

Rodney Peterson, Security Task Force Coordinator of EDUCAUSE serves as a Co-Chair of the Awareness Task Force's education working group, and will tell you about the great work that is going on in that field. He, along with Co-Chair Jim Teicher, Executive Director of CyberSmart!, produced a detailed plan with specific actions by set dates.

For state and local governments, we gathered a group of talented and dedicated leaders committed to raising cyber security awareness in this target market. Among the many accomplishments this group made were: the recommendation to establish a

national awards program, in conjunction with DHS, to recognize outstanding achievement from teams of state and local government information security specialists; the development of web-based cyber security tutorials; and the compilation of best practices tools for state and local governments. The working group also has identified distribution channels for this compilation.

One of the most rewarding aspects of leading the awareness segments of both of these efforts was seeing the tremendous interest in our work. School boards, teacher's unions, Fortune 500 firms, and small businesses all contributed to our efforts and will be essential to our ultimate success. And there is no better manifestation of this commitment than the fact that our next National Cyber Security Summit Awareness and Outreach Task Force Meeting is set for Friday, April 30.

Mr. Chairman, thank you again for this opportunity. I would be happy to answer any questions you or your committee might have.