AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY AND CONSUMER DATA: WHAT'S AT RISK FOR THE CONSUMER?

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2003

Serial No. 108–52

Printed for the use of the Committee on Energy and Commerce



Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

90–728PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
Vice Chairman
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California

DAN R. BROUILLETTE, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
Vice Chairman
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
ERNIE FLETCHER, Kentucky
MIKE FERGUSON, New Jersey
DARRELL E. ISSA, California
C.L. "BUTCH" OTTER, Idaho
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
HILDA L. SOLIS, California
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
JIM DAVIS, Florida
PETER DEUTSCH, Florida
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

Page

Testimony of:

Ansanelli, Joseph G., Chairman and CEO, Vontu, Inc 48
Burton, Daniel, V.ice President, Governmental Affairs, Entrust Technologies 52
Charney, Scott, Chief Trustworthy Computing Strategist, Microsoft Corporation 30
Davidson, Mary Ann, Chief Security Officer, Oracle Corporation 43
Morrow, David B., Managing Principal, Global Security and Privacy Services, EDS 37
Schmidt, Howard A., Vice President, Chief Information Security Officer, eBay Inc 23
Swindle, Hon. Orson, Commissioner, Federal Trade Commission 16
Thompson, Roger, Vice President of Product Development, PestPatrol, Inc 58

CYBERSECURITY AND CONSUMER DATA: WHAT'S AT RISK FOR THE CONSUMER?

WEDNESDAY, NOVEMBER 19, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:10 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Shimkus, Shadegg, Pitts, Bono, Issa, Schakowsky, Towns, Davis, Green, and McCarthy.

Staff present: Ramsen Betfarhad, policy coordinator and majority counsel; Jill Latham, legislative clerk; Jon Tripp, deputy communications director; David Cavicke, majority counsel; and David Nelson, minority counsel.

Mr. STEARNS. Good morning. Welcome to the Subcommittee on Commerce, Trade, and Consumer Protection's hearing on cybersecurity and consumer data. I am pleased that we are joined this morning by a group of distinguished witnesses. And all of us look forward to your testimony.

On November 15, 2001, nearly 2 years ago to the day, the subcommittee held a hearing entitled, "Cybersecurity: Private Sector Efforts Addressing Cyber Threats." The focal point of that hearing, as it is with this hearing, was cybersecurity as it related to consumer data used in stream of commerce.

We are fortunate that three of our witnesses, Ms. Davidson, Mr. Schmidt, and Mr. Morrow, all of whom testified at the hearing 2 years ago, have joined us today to reflect on what has transpired with regard to cybersecurity in the last 2 years. Normally you don't have people back to give you a little post-analysis. So we are very fortunate to have that.I am confident their insights, along with the testimony of the other witnesses, will be particularly helpful to our better understanding the issue, its evolution, and what we believe is its increasing significance.

The subcommittee's hearings 2 years ago was held in the shadow of the tragic events of September 11, when we as a Nation, it seemed, had become obsessed with security. Of course, that was and is understandable. Yet the problem that gave rise to cybersecurity concerns that predated September 11, in just the years 2000 and 2001, as a result of only three cyberattacks—the "I Love You" and "Code Red" viruses and the February 2000 de-

nial-of-service attacks—the media reported losses in excess of $10 billion.

The number of cyberattacks, as reported by the Computer Emergency Response Team, CERT, at the Carnegie Mellon University, was expected to nearly double in 2001 from 2,000 to 40,000.

Now, fast forward 2 years. In 2003, the "SQL Slammer" worm disrupted computers around the globe. And during the attack, half of all Internet traffic was being lost. The SoBig.F virus clogged e-mail boxes and networks around the world, and became the fastest spreading virus on record, infecting 1 in 17 e-mails at its peak.

Showing a bit of humor, the creator of the Blaster worm, which caused some 500,000 computers running Windows to crash, targeted the Microsoft Web site from which users could download the program and the patch to protect their vulnerability with Microsoft Windows code, the very weakness in Windows that the worm itself was exploiting.

The virus and worm attacks of 2003 did bring about disruptions, such as the SQL Slammer worm, knocking out Bank of America's ATM machines for a while, but overall they did little reported damage. Although the ultimate objective of the SoBig.F virus is not known, the 2003 vintage of viruses and worms, like most of the ones that preceded them, did not have a malicious or destructive payload. If they did, their impact would have been very, very different. These viruses and worm attacks are external attacks to the networks, and, as such, according to some estimates, only represent 30 percent of computer attacks. The remaining 70 percent of the attacks are carried out from within the corporate firewalls.

Those attacks or security breaches taking place within the corporate firewalls, many argue, are the most costly and, of course, the least reported. I raise the issue of virus and worm payload within corporate firewall breaches, because one key question I want answered today is "What are the real risks and costs to consumers from cybersecurity breaches, and what poses the most risk to cybersecurity?"

One response to breaches in cybersecurity by industry and government alike has been increased spending on security technologies. UBS Warburg estimates that such spending will increase from $6 billion in 2001 to over $13 billion in the year 2003.

Meanwhile, other data suggests that companies spend less than just 3 percent of their technology budget on security. The technology budgets tend to be around 3 percent of revenues. So why are these expenditures so low? Some argue because there is no real understanding of quantifiable cost associated with cybersecurity breaches, even among senior managers. Is this true? This is another question for the panel to consider.

Finally, many argue that cybersecurity is not just a technological problem and thus can't be solved by adding new and improved technologies defending against cyberattacks, but, rather, they argue that it is as much a governance or management issue as it is a technological problem. Strategic decisions, such as deciding the appropriate balance between cost and risk, are ones that only senior managers can take. And without a clear mandate from the top management, cybersecurity measures will be disregarded as just simply nuisances by rank-and-file employees.

Moreover, it appears that there is increased management participation mostly when it is mandated either directly or indirectly by government regulations. For example, the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act, or enforcement actions by the Federal Trade Commission.

I want to know, are these observations accurate? If so, is there an optimum role for the Federal Government to play when it comes to protecting consumers from cybersecurity threats?

With that, I conclude my opening statement and welcome the ranking member for her opening statement.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, for conveying this important hearing today. Cybersecurity is one of those words that have recently entered our lexicon. Most people are probably confused, as I was, the first time they hear or see it in print. There are no doubt several interpretations of the word. It is one of those things like electricity or television signals that we all hope someone else understands enough to assure its availability.

Before widespread viruses and ID theft became somewhat of a norm, we were able to take cybersecurity for granted. Of course, it should be safe to operate a home computer or a Palm Pilot. Unfortunately more and more Americans, a disproportionate share in and around Chicago, by the way, have come to a very personal understanding of how vulnerable our information technology, storage, and transmittal systems are.

No longer is cybersecurity something over which just government and corporate technicians fret. Life savings now disappear before victims are even aware that there is a threat to the security of their personal and financial information. Highly sensitive personal information is available for sale without the knowledge, much less the consent, of targeted individuals.

Americans expect that their government and the private sector institutions they rely upon for financial and other services will protect their privacy, and that those they rely on for cybersecurity will do their job. It is becoming increasingly apparent that consumers are not being adequately protected.

Estimates of the economic impact of cybercrimes on society vary widely. One of our witnesses will tell us that identify theft alone totaled $24 billion last year, and is expected to escalate to $73 billion by the end of this year. If he is correct, this means that identity theft will cost Americans more, perhaps much more, than the authorized cost of the war in Iraq.

Another witness tells us that 1 in 10 Americans has been victimized by identify theft. Each of these heists is estimated to cost nearly $10,000; clearly this problem is reaching epidemic proportions.

Added to the economic cost is the loss of our invaluable privacy. We are all aware of the Orwellian dangers that may flow from personal information that the government can tap, using sophisticated technology. What many of us do not adequately understand is the danger of intrusive prying by private interests. The expropriation of commercially useful data from each and every one of us that accesses the Internet from a computer where personal information is stored is a continuous process. And, of course, there is no reason

to believe that firms interested in selling us something are the only ones looking.

I look forward to the testimony of the Federal Trade Commission regarding what the Federal Government is doing to control this electronic crime spree. I hope in the future we can also hear from the Justice Department or the agencies that regulate financial institutions, because it is my understanding that much, if not most, of identify theft is perpetrated by employees of banks, insurance companies, and the like.

I would have liked to hear directly from those private institutions as well. Nonetheless, Mr. Chairman, I am looking forward to hearing from the witnesses you have assembled. I am sure they will be able to give us a sufficiently comprehensive picture of the problems with our cybersecurity systems from which we can fashion whatever policy changes may be necessary to protect the privacy, pocketbook, and safety of our constituents.

And, Mr. Chairman, I look forward to working with you, as always, to end this epidemic. I look forward hearing from each of our witnesses, and I thank them for taking time to share their expertise with us today.

Mr. STEARNS. I thank the gentlelady.

The gentlelady from California, Ms. Bono.

Mrs. BONO. Good morning, and thank you, Mr. Chairman. I look forward to hearing from your colleagues and the witnesses on the issue of cybersecurity as it relates to consumers.

Cybersecurity and the protection of consumer data is a very real issue that the government, businesses, and consumers alike must acknowledge and respond to. Of course, there are many things that consumers can do to protect themselves.

Antivirus software and patches are regularly available for downloading and updating. Moreover, one should always be cautious while downloading software. Consumers should avoid opening e-mails from strangers and should be hesitant to disclose personally identifiable information over nonsecure sites.

However, the methods of hacking into computers and data bases are just as evolving as the technologies on which they reside and function. Recently I introduced H.R. 2929, also known as the Safeguards Against Privacy Invasions Act, or the Spy Act. This bill aims to put consumers in the loop. Unfortunately, consumers regularly and unknowingly download software programs that have the ability to track their every move.

Consumers are sometimes informed when they download such software. However, the notice is buried deep inside multi-thousand-word documents that are filled with technical terms and legalese that would confuse even a high-tech expert.

Many spyware programs are purposefully designed to shut off any antivirus or firewall software program it detects. The Spy Act would help prevent Internet spying by requiring spyware entities to inform computer users of the presence of such software, the nature of spyware, and its intended function.

Moreover, before downloading such software, spyware companies would first have to obtain permission from the computer user. This a very basic concept. The PC has become our new town square and global market as well as our private data base. If a consumer

downloads software that can monitor the information shared during transactions for the sake of the consumer as well as e-commerce, it is imperative that the consumer be informed of whom he or she is inviting into their computer and what he or she is capable of. After being informed, the consumer should have the chance to decide whether to continue with that download.

Since the introduction of H.R. 2929, I have had the opportunity to speak with many different sectors of the technology industry and retail businesses that operate on the Internet. Through these discussions I have received meaningful feedback, and I am currently working on refining H.R. 2929. Once installed on computers, some spyware programs—like viruses embedded among code for other programs—in effect how these programs function on the users computer.

Additionally, spyware is becoming more and more difficult to detect and remove. Usually such programs are bundled with another unrelated application that cannot be easily removed, even after the unrelated application has been removed.

According to a recent study, many problems with computer performance can be linked in some way to spyware and its applications. Additionally, some computers have several hundred spyware advertizing applications running, which inevitably slow down computers and can cause lockups. If you have spyware on your computer, you most likely are getting more pop-up advertisements than you would have if you have had no such software on your computer.

Moreover, the advertisers may not always be forthcoming. Many times spyware entities contract with companies to post advertisements and, in turn, post such advertisements on the Web sites of competitors. The result is confusion. In other words, while visiting the Web site for Company A, you may be browsing to purchase a product. However, while browsing, a pop-up link may appear, informing you of a great sale. Under the impression that you are looking at a link for Company A, you may purchase the product, all the while uninformed that the product was purchased via a pop-up link from Company B. I have often thought that this would be a very effective campaign tool, too, to put out a link and have someone go to my opponent's Web site and my Web site pops up.

All of these consumer disadvantages can be decreased or eliminated if disclosures surrounding spyware are required and enforced. If consumers are informed about spyware, chances are they will not choose to download the software. Upon choosing not to download software, consumers' computers will run more efficiently, their antivirus programs and firewalls will function better, they can decide which information to share and not share, and consumers will not be deceived into buying a product or service from unknown entities or voting for our opponents.

Thank you, and I look forward to hearing from the witnesses on the issue.

Mr. STEARNS. I thank the gentlelady.

Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman. I thank you and our ranking member for holding this important hearing on cybersecurity and its impact on consumers.

The proliferation of Internet-based services and commerce has dramatically changed the world we live in, and many of these changes have been for the better, with consumers able to make almost any purchase imaginable on line. Unfortunately, these computing advances also create a fertile ground for fraudulent activities and thus increase the pressing need for computer security.

The problems are coming from all directions. We have viruses, computer worms that are attempting to swarm our networks and are causing terrible harm to computer users and billions in damages to U.S. Businesses. We have unsolicited e-mails taking over our in-boxes, spam that at the very least is an annoyance and at worst is helping to transmit these computer viruses and deliver pornographic e-mails to our children.

Mr. Chairman, if I could ask unanimous consent to put in an article from Business Week that was published on August 12 about the unholy matrimony, spam versus virus.

Mr. STEARNS. By unanimous consent, so ordered.

[The article referred to follows:]

[Business Week—August 12, 2003]

UNHOLY MATRIMONY: SPAM AND VIRUS

By Jane Black

Their common goal is subterfuge, and by combining their strategies, they could make today's junk e-mail look like a mere nuisance

In June, half of all e-mail was spam—those annoying unsolicited messages that hawk everything from porn and Viagra to mortgage-refinancing deals and weight-loss patches. But if you think spam is out of control, prepare yourself. It could get a lot worse.

Over the past few months, e-mail security companies have seen mounting evidence that spammers are using virus-writing techniques to assure that their sales pitches get through. At the same time, intrepid virus writers have latched onto spammers' trusty mass-mailing techniques in an effort to wreak widespread digital mayhem. "What we're seeing is the convergence of the spammer and the malicious code writer," says David Perry, global director of education at antivirus company Trend Micro (TMIC).

RELAY STATIONS. Witness the recent spread of a virus known as Webber, which was discovered on July 16. It carried the subject line "Re: Your credit application." Users who opened the attachment downloaded a malicious program that turned a home PC into a so-called open relay server, which allows a third party to send or receive e-mail—including spam—remotely from that PC. Spammers are notorious for using open relays to hide their identities. According to British e-mail security company MessageLabs, 70% of spam comes through open relays.

Then there's Sobig.E, a virus that grabs e-mail addresses from several different locations on a PC, including the Windows address book and Internet cache files. Sobig.E then tries to send a copy of itself to each address. It also uses one of the stolen addresses to forge the source of the message, so that it appears to come from someone else. MessageLabs believes Sobig.E is a spammers' virus designed to harvest legitimate e-mail addresses from users' computers.

So far, no concrete evidence shows any home PCs that have been infected by either Webber or Sobig.E have been used to send spam. But experts fear that the two viruses could be "spam zombies," programs that will lie in wait on a PC until called on by the spammer to send out millions of untraceable e-mails.

"I LOVE YOU" MORE. The convergence of spam and malicious code makes sense, says Chris Miller, Symantec's (SMYC) group product manager for enterprise e-mail security. "They have a common goal—to do what they're doing without being seen," Miller says.

Virus writers and spammers send out their messages from illegitimate e-mail accounts, never from the ISPs where they are registered. It isn't hard to see where the union of these two insidious groups' techniques might lead. Using such weapons as Sobig.E and Webber, spammers can hijack a user's address book, then use the PC to send out hundreds, even thousands, of junk messages.

And virus writers can use mass-mailing techniques to spread malicious code even faster than before. The destructive "I Love You" virus of 2000 was originally sent to a small number of people. Within days it had affected tens of millions of computers and caused damage worth hundreds of millions of dollars. Imagine if, like spam, it had originally been mailed to a half-million computers.

Security experts cite other recent examples of spam-virus convergence:

- Key-logger Trojans. In May, 2003, a major food-manufacturing company received a spam e-mail that, when viewed in a preview pane in Microsoft Outlook, showed a message that appeared to be an opportunity to sign up for a newsletter. First, though, the message asked the recipient to verify their e-mail logon ID and password. That information was collected by the key-logger code and then sent to the spammer, who could then log into the user's e-mail at any time and search for valuable information.
- Drive-by downloads. Recent spam sent to a major airline manufacturer led unsuspecting users to Web pages where spying software was secretly downloaded without the user's knowledge. So-called spyware monitors a user's activity on the Internet and transmits that information to someone else, usually an advertiser or online marketer. Spyware can also gather information about e-mail addresses, passwords, and credit-card numbers. Drive-by downloads can be done without either notifying the user or asking permission because many users accept such a download without question, thinking it's a normal function of the Web site.

CALL IT "MALWARE." According to the strictest definitions, key loggers and drive-by downloads aren't viruses, which are programs that replicate themselves. (If you've seen The Matrix Reloaded, think of the way Agent Smith makes infinite copies of himself to try to destroy Keanu Reeves' Neo.) A Trojan is a program that rolls into your computer unannounced, then persuades the computer to launch it through fraud.

As spam and malicious code converge, however, such definitions are becoming less useful. That's why experts like Trend Micro's Perry are now looking at a broader term—"malware"—to describe any program with malicious intent. "With traditional hackers, the motivation has always been to prove that you're a rad dude," Perry said in a phone interview from the Las Vegas hacker convention DefCon. "But when we start seeing these techniques used for commercial gain like spam, it's going to get a whole lot more serious." Cybersurfers, beware.

Mr. GREEN. Thank you, Mr. Chairman. We can all agree that spam is a serious problem that both Congress and the private sector should address quickly, and I hope that Congress will act before the end of the session to enact the Wilson-Green Antispam Act of 2003, which is the strongest antispam bill in Congress.

And, Mr. Chairman, again, I would like to ask unanimous consent to place into the record a letter by the Internet Committee of the National Association of Attorney Generals that talks about the Senate bill that passed and the need for strong legislation.

Mr. STEARNS. By the unanimous consent, so ordered.

[The letter follows:]

INTERNET COMMITTEE
OF THE NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

Consisting of the Chief Legal Officers
of California, Kansas, Maryland, Nevada, Texas, Vermont, Virginia, and Washington



November 4, 2003

The Honorable J. Dennis Hastert
Speaker of the House
235 Cannon House Office Building
Washington, DC 20515

The Honorable Nancy Pelosi
House Minority Leader
2371 Rayburn House Office Building
Washington, DC 20515

The Honorable W.J. "Billy" Tauzin
Chairman, House Energy
and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable John D. Dingell
Ranking Member, House Energy
and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable F. James Sensenbrenner
Chairman, House Judiciary Committee
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member, House Judiciary Committee
2138 Rayburn House Office Building
Washington, DC 20515

Re: S.877, The CAN-SPAM Act of 2003

Dear Representatives:

The CAN-SPAM Act of 2003, which recently passed out of the Senate and is now in the House of Representatives for consideration, is a laudable effort at dealing with the enormous problem of spam. We are encouraged that Congress has recognized the importance of the issue and the need for legislation. A majority of the states have passed statutes regulating spam, and we believe that these laws should complement a strong federal law.

Because it passed so quickly through the Senate, we have only just now had the opportunity to review S. 877, as amended by the Senate. Unfortunately, in its current form, the Bill creates so many loopholes, exceptions, and high standards of proof, that it provides minimal consumer protections and creates too many burdens for effective enforcement. Its substantive protections are weak, as are its damage provisions. It preempts stronger state laws. The defenses it provides for would-be violators virtually assure that it will engender litigation, rather than deter unlawful conduct. We respectfully request that you not move forward with S. 877 and ask that you consider a bill that provides more protections for consumers and businesses.

The following is a breakdown of our concerns about the Bill. This list is not exhaustive, but presents what we see as the major issues:

1. Section 105(a)(2) prohibits deceptive subject headings but creates standards of knowledge and materiality that are unprecedented in consumer protection law. The provision requires that a person "knows" the subject heading "would be likely to mislead a recipient, acting reasonably under the circumstances about a material fact regarding the contents or subject matter of the message." Consumer protection law only requires a capacity or tendency to deceive the recipient in order to show a violation. Requiring a showing of knowledge and materiality creates a barrier to enforcement where none currently exists.

This heightened knowledge standard is also found at Section 103(13) of the legislation which concerns liability for a person who "procures" the services of a spam sender to initiate an unlawful message. The term "procure" requires that an individual know or consciously avoid knowing he is hiring someone to send an unlawful spam message. Again, this knowledge standard exceeds what is found in other consumer protection statutes.

2. Section 103(2)(A) defines a "commercial electronic mail message" as having the "primary purpose" of promoting a commercial product or service. This language creates a loophole for spammers who may argue the primary purpose of their email is something other than advertising. It creates an unnecessary defense and narrows the category of commercial email that consumers should be allowed to opt out of.

3. Section 105(a)(3)(B) permits the sender to create a menu approach to opting out. By permitting the sender to create this menu approach, the ease, utility, and understandability of the opt out is compromised. Consumers will not be able to easily elect to stop receiving emails – they will have to decide, based on the sender's potentially confusing menu of choices, what they wish to opt out of, and if they want to receive some but not all unsolicited email. The option of a total opt-out, while required in the bill, can easily be buried in text by the sender.

4. Section 105(a)(3)(C) provides that if a sender's electronic mail address or other mechanism is "unexpectedly and temporarily unable to receive" an opt-out message, the sender will not be out of compliance with the law. This creates a big loophole, since spammers are always unable to receive messages right after their spam is sent out – their mailboxes are always full at that point. And that is precisely when most opt-out requests are made.

5. Section 105(a)(4)(A) prohibits a sender's initiation of email to a recipient who has opted out "more than 10 business days after the receipt of such request." While a short period of time for compliance may be reasonable, 10 business days is simply too long. The following section, Section 105(a)(4)(C) creates an even bigger loophole. It provides that persons who act on behalf of the original sender are only liable if they "know or consciously avoid knowing" of the recipient's opt-out to the original sender. As a practical matter, the middlemen, or "spam houses" in the industry, will say they simply didn't know a recipient had opted out, and thereby escape liability by insulating themselves from knowledge.

6. Section 105(b)(B)(1)(A) prohibits "harvesting" of email addresses (when a spammer captures email addresses off of third-party websites and chatrooms) and "dictionary attacks" (when a spammer generates email addresses through an automated means). These are only deemed aggravating violations of other violations of the statute, and cannot be independent bases for liability. Given that these practices significantly affect Internet Service Providers and other online businesses, there should be independent causes of action for both.

7. Section 105(c) provides that spammers may avoid liability if they can show they implemented "reasonable practices" to avoid violations and that they made "good faith" efforts to

comply. This creates a defense that is unprecedented in consumer protection law and also creates an additional barrier to enforcement.

8. Section 106(a) creates liability for those whose products are sold by a spammer when that person "knows or should have known" unlawful spam was sent on his behalf, he received economic benefit from the spam, and took no reasonable action to prevent it or detect it and report it to the FTC. Liability for this section is only limited to those who own 50% or more of the merchant business or those who have actual knowledge of the violation. It is seemingly at odds with other provisions for liability in the bill, including those which define the "initiator" of an email as a person who procures a sender's services to send an email (i.e., a merchant). According to these provisions, at Section 105, liability falls on those who procure such services in the same manner it falls on other violators. In contrast, Section 106(a) essentially forecloses any liability for merchants, except in extremely limited circumstances.

Section 106(a) also limits enforcement ability exclusively to the FTC, which is different from other parts of the statute that allow for state and ISP enforcement.

9. Section 107(e)(2) limits the recovery of states for violations of the bill to $100 for violations involving misleading header information and $25 for all other violations. Additionally there is a cap on overall damages of $1,000,000 for any violations other than misleading headers. Neither of these amounts will act as a significant deterrent to spammers who will simply see it as a "cost of doing business." States may have a difficult time proving with particularity how many spams were sent to their citizens and statutory damages will likely be minimal in those circumstances. Internet Service Providers are hampered by similar limits at Section 107(f).

10. Section 108(b) preempts many state laws which regulate the use of electronic mail. Though states' statutes prohibiting falsity or deception in commercial email are not preempted, numerous states have taken a broader approach to regulation. Some states require labeling, others provide for specific disclosures within the body of the email. At least one state statute provides that before a spammer can send email, the recipient must opt in to receiving it. The preemption in S.877 effectively negates these statutory schemes and leaves a much weaker set of provisions in their place. Given the concerns we have described above, we strongly oppose the bill's preemption provisions.

In conclusion, while we support the efforts of Congress to address the issue of spam in order to protect consumers and businesses, we believe that S.877 lacks the necessary elements to reach that goal. We would welcome the opportunity to work with the House in assuring that what is ultimately passed will be effective. We look forward to working with you and encourage you to contact us directly.

Sincerely,

Attorney General Christine O. Gregoire
Attorney General of Washington
Chair, NAAG Internet Committee

Attorney General Bill Lockyer
Attorney General of California
NAAG Internet Committee

Attorney General Phil Kline
Attorney General of Kansas
NAAG Internet Committee

Attorney General J. Joseph Curran Jr
Attorney General of Maryland
NAAG Internet Committee

Attorney General Brian Sandoval
Attorney General of Nevada
NAAG Internet Committee

Attorney General Greg Abbott
Attorney General of Texas
NAAG Internet Committee

Attorney General William H. Sorrell
Attorney General of Vermont
NAAG Internet Committee

Attorney General Jerry W. Kilgore
Attorney General of Virginia
NAAG Internet Committee

cc:

House Energy and Commerce Committee

Michael Bilirakis
Joe Barton
Fred Upton
Cliff Stearns
Paul E. Gillmor
Jim Greenwood
Christopher Cox
Nathan Deal
Richard Burr
Edward Whitfield
Charles Norwood
Barbara Cubin
John M. Shimkus
Heather A. Wilson
John B. Shadegg
Charles Pickering
Vito Fossella
Roy Blunt
Steve Buyer
George P. Radanovich
Charles Bass
Joseph R. Pitts
Mary Bono
Greg Walden
Lee Terry
Ernest Lee Fletcher
Michael A. Ferguson
Michael J. Rogers
Darrell Issa
C.L. Otter

Henry A. Waxman
Edward J. Markey
Ralph M. Hall
Rick Boucher
Edolphus Towns
Frank Pallone, Jr.
Sherrod Brown
Bart Gordon
Peter Deutsch
Bobby Rush
Anna Eshoo
Bart Stupak
Eliot Engel
Albert Wynn
Gene Green
Karen McCarthy
Ted Strickland
Diana L. DeGette
Lois Capps
Mike Doyle
Chris John
Thomas H. Allen
Jim Davis
Janice D. Schakowsky
Hilda L. Solis

House Judiciary Committee

Henry J. Hyde
Howard Coble
Lamar S. Smith
Elton Gallegly
Bob Goodlatte
Steve Chabot
William L. Jenkins

Howard L. Berman
Rick Boucher
Jerrold Nadler
Bobby Scott
Melvin L. Watt
Zoe Lofgren
Sheila Jackson Lee

Chris Cannon	Maxine Waters
Spencer Bachus	Marty Meehan
John N. Hostettler	William Delahunt
Mark Green	Robert I. Wexler
Ric Keller	Tammy Baldwin
Melissa A. Hart	Anthony D. Weiner
Jeff Flake	Adam Schiff
Mike Pence	Linda T. Sánchez
Randy Forbes	
Steve King	
John R. Carter	
Tom Feeney	
Marsha Blackburn	

Mr. GREEN. Thank you, again, Mr. Chairman.

When we investigate cybersecurity, however, we must also consider the increasing troubles and problem of identity theft. According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all 50 States. With simple personal information such as name, Social Security number, or credit card number, identity thieves can commit fraud or other crimes in our name.

The implications for victims of identify theft can't be overexaggerated. They can easily include damaged credit records, unauthorized credit card charges, and bank withdrawals, not to mention the months or even years that it takes for victims to restore their good names and credit records.

The magic question remains, how can we prevent these computer-related security problems that seem to be spiraling out of control? With the increased organization, efficiency, and productivity that computer systems offer, it is safe to say that our dependence on computers will continue to rise; therefore, we must ensure that we take the appropriate precautions to ensure that any information stored in or transmitted through computers, be it personal, medical, or financial, is secure.

We also need to examine the extent to which the Federal Government and other law enforcement mechanisms can help solve this problem. By some estimates, less than 30 percent of computer attacks come from outside of a company or computer system. That being said, I think we have to work with the private sector to take a hard look at the practices companies are putting in place to combat attacks within their own firewall.

I am also interested to hear our witnesses' experience with cybersecurity and learn their opinions on how best we can go about solving these problems. And, again, I would like to thank our panel today, and look forward to their testimony.

Thank you, Mr. Chairman and Ranking Member Schakowsky.

Mr. STEARNS. Thank you.

Mr. Pitts.

Mr. PITTS. Thank you, Mr. Chairman. And thank you for convening this important hearing on cybersecurity.

Rapid advances in technology are greatly impacting the lives of every American. Computer software, information systems, and cybernetworks are revolutionizing the way that we communicate, and the way we conduct business and provide services. And while

there is a lot of good in the advances, there is also great potential for harm.

Technology is a cat-and-mouse game. Each advancement of technology leads to an exploitation that we must vigilantly guard against, and the hearing this morning takes a look at the myriad threats to cybersecurity. One area that I am greatly concerned about is the development of peer-to-peer software.

Peer-to-peer software allows individuals to download and trade files, many of which are illegal, with one another. It has also become the latest vehicle that pedophiles use to exploit and abuse innocent children by distributing child pornography. And peer-to-peer software can cause any personal information stored in a computer, such as financial or medical records, to be inadvertently shared with anyone else with the same software.

And that is why my colleague Chris John and I introduced H.R. 2885, "The Protecting Children from Peer to Peer Pornography Act."

Mr. Chairman, I appreciate your interest in this issue. It is my hope that we can have a hearing in the near future dedicated to taking a closer look at this dangerous new software that threatens our children or a person's privacy and our cybersecurity in general.

Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

The gentleman from New York, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman.

The Internet will never reach its fullest potential unless consumers feel comfortable and confident while surfing the Web and partaking in e-commerce. How can we ask citizens to put personal information, such as credit cards, PIN numbers, onto the computer if they are worried about issues such as identity theft, spam, or other privacy protections?

It seems that every time we turn around there is a new virus harming commerce on the Internet, and the most pressing of these data and privacy abuses is what has come to be known as spyware. Spyware is a particularly dangerous threat to the future of e-commerce and Internet consumer confidence.

Many times consumers do not even know what this software—which can track all movements on a computer, copy keystrokes, and open security holes in networks—is open on their system, much less have the knowledge it takes to get them removed.

It should also be noted that many of the peer-to-peer programs suggested Kazaa and Morpheus are funded largely by allowing these spyware companies to piggyback on their network, allowing for corporate entities to gain information about our children and their on-line habits.

I am proud upon the lead Democratic sponsor of H.R. 2929, the Safeguard Against Privacy Invasion Act, with my friend from California, Mrs. Bono. This bill will ban these programs from being downloaded from the Internet to unknowing consumers. It is a commonsense approach to privacy protection, and I would like to thank the many members on both sides of the aisle from this committee who have chosen to cosponsor the bill with us, and look forward to working closely with the leadership to ensure its passage through the committee.

On that note, Mr. Chairman, I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman.

Mr. Shimkus.

Mr. SHIMKUS. Thank you, Mr. Chairman, and I will be brief.

I always want to take the opportunity to, especially in consumer protection that deals with the Internet and cybersecurity, to continue to mention .kids.us as a place safe for kids, that was passed into law, signed by the President, and now we have groups that are using it: Smithsonian.kids.us, it is safe, no hyperlinks, no chatrooms for kids under the age of 13.

And so I use the bully pulpit here to continue to help build interest and movement for people to take use of .kids.us.

Other than that, Mr. Chairman, I know we have got a great panel of people testifying. I want to get to that. Thank you for the time. And I yield back.

Mr. STEARNS. I thank the gentleman.

The gentlelady from Missouri.

Ms. MCCARTHY. Mr. Chairman, I want to thank you for pulling together such a distinguished panel of experts for our work today. I am going to put my remarks in the record so that we can get on learning about the wisdom that is here to be shared.

Mr. STEARNS. I thank the gentlelady.

And the vice chairman of the committee, Mr. Shadegg.

Mr. SHADEGG. Thank you, too, Mr. Chairman. I too want to thank you for holding this important hearing today and for putting together a tremendous panel for us to learn from.

And I do want to mention that both as a member of this subcommittee, and as a member of the Select Homeland Security Committee, I worry deeply about these issues. I have devoted a great deal of time to them, having written in 1998 the Identity Theft and Assumption Deterrence Act, which made identity theft a Federal crime for the first time.

We have already heard here this morning the degree to which millions of Americans are victimized by that crime, and that we are losing billions of dollars to it.

The Fair Credit Reporting Act, which is now in conference, includes some important provisions to deal with that issue. But there is much more we can do. And I appreciate, Mr. Chairman, your holding this hearing, and I look forward to the testimony of the witnesses.

Mr. STEARNS. I thank my colleague.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Mr. Chairman, Thank you for calling this important hearing today.

Cyber security is a very serious concern in today's digital world, and as our global economy and all of our lives rely more and more on computers, it will become essential that we ensure that our nation's computers—corporate, government, and personal computers—are safe from the hackers and other malefactors in the digital environment. We've learned in the last few years how much damage viruses and worms, such as "Sobig.F" and "Blaster," can do to our computer infrastructure. In fact, the *New York Times* estimated that the cost of the "I Love you" virus alone—which seriously affected this House and this Committee—may have reached as much as $15 Billion.

Computers affect almost every aspect of our daily lives. From our computers at home and our personal e-mail accounts, to the daily work of the public and private

sectors, the role of computers in our society is so ubiquitous as to go almost unnoticed at times. The security of these systems however cannot go unnoticed. Not only can the e-mail system of the House of Representatives be hindered or disabled, but one shudders to think of the damage that could be done to countless consumers if someone was able to infiltrate one of the many enormous databases in this country and steal the personal information—from credit card numbers to music preferences—of millions of Americans.

This kind of theft and misuse of personal data is not yet a widespread problem, but unless we all facilitate and encourage open discussion about how we best combat the bad actors, we will only see these problems grow. Most computer scientists don't say "if" when discussing this possibility, they say "when." They believe that a truly debilitating virus will inevitably make its way around the Internet sometime in the relatively near future. Companies must take a preventive approach when looking at solutions to security problems. They must realize that, as the old adage says, "An ounce of prevention is worth a pound of cure." We must combat technology with technology. Investment must be made in the security of vital and sensitive systems, in order to ensure the confidence of the American people in the retail, banking, and health care computer systems they depend upon.

But simply investing in technology to combat viruses is not enough. In the end, the private sector and the American people must work in concert to best protect the computers and networks we all use. The private sector needs to reevaluate its vulnerabilities as well as its current security priorities. The public needs to be better educated about anti-virus software and personal firewalls for their home computers, as well as the insidious "SpyWare" technology that can monitor individuals' computers and their actions on the Internet. I know the gentlelady from California, Ms. Bono, has introduced a bill—H.R. 2929, "The Safeguard Against Privacy Invasions Act"—that attempts to deal with this concern, and I look forward to working with her on the bill to try to prevent these intrusions.

In the end, Mr. Chairman, it seems that the genie is out of the proverbial bottle, and this problem is not going to go away on its own. It is up to all of us to work together to safeguard our computer infrastructure to prevent the next serious virus from becoming a nationwide, indeed even a worldwide problem.

Thank you, and I yield back the balance of my time.

Mr. STEARNS. And with that, we will start with the panel and welcome the Honorable Orson Swindle, the Commissioner of the Federal Trade Commission; Mr. Howard Schmidt, Vice President, Chief Information Security Officer of eBay; Mr. Scott Charney, Chief Trustworthy Computing Strategist from Microsoft Corporation; Mr. David Morrow, Managing Principal, Global Security and Privacy Services; Ms. Mary Ann Davidson, Chief Security Officer, Oracle Corporation; Mr. Joseph G. Ansanelli, Chairman and CEO of Vontu, Incorporated; Mr. Daniel Burton, Vice President of Government Affairs, Entrust Technologies; and Mr. Roger Thompson, Vice President of Product Development, PestPatrol, Incorporated.

And we will let Commissioner Swindle start. We will go from my right to my left. I welcome you.

STATEMENTS OF HON. ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION; HOWARD A. SCHMIDT, VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER, eBAY INC.; SCOTT CHARNEY, CHIEF TRUSTWORTHY COMPUTING STRATEGIST, MICROSOFT CORPORATION; DAVID B. MORROW, MANAGING PRINCIPAL, GLOBAL SECURITY AND PRIVACY SERVICES, EDS; MARY ANN DAVIDSON, CHIEF SECURITY OFFICER, ORACLE CORPORATION; JOSEPH G. ANSANELLI, CHAIRMAN AND CEO, VONTU, INC.; DANIEL BURTON, VICE PRESIDENT, GOVERNMENTAL AFFAIRS, ENTRUST TECHNOLOGIES; AND ROGER THOMPSON, VICE PRESIDENT OF PRODUCT DEVELOPMENT, PESTPATROL, INC.

Mr. SWINDLE. Thank you, Mr. Chairman. Mr. Chairman, members of the subcommittee, I appreciate the opportunity to present the Commission's views on Cybersecurity and Consumer Data: What is at risk for the consumer?

At the outset, I believe that it is important that we not lose sight of the forest for the trees. Cybersecurity is a vast issue that faces many threats, and the challenges that the Commission faces in protecting consumers in cyberspace are numerous. The Commission takes action to protect consumers from fraud, whether they are individuals or companies who engage in identity theft, use a pretext to obtain personal information, employ deceptive spam to trick consumers into providing personal and financial information (phishing), misrepresent the sender of spam to misdirect the "remove me" request to an innocent third party (spoofing), or exploit computer system vulnerabilities in order to extort money from consumers (D-Square Solutions).

Consumers are also placed at risk by their own conduct, such as through peer-to-peer file-sharing or failing to use firewalls and antivirus software. While there are many challenges to cybersecurity, I will focus my remarks on companies who obtain and control consumer information.

The Commission addresses information security concerns through aggressive law enforcement actions, consumer and business education, and international cooperation. Through these efforts we strive to enhance the security of information systems and networks and bring attention to the fact that all users of information technology, that is, government, industry, and the general public, must play a role in this effort.

If companies fail to keep their express and implied promises to protect sensitive information obtained from consumers, then those promises are deceptive. The Commission has brought enforcement actions against such companies for violating Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices.

Three of these Commission cases illustrate some important principles. The case against Eli Lilly demonstrates that a company's security procedures must be appropriate for the kind of information it collects and maintains. Despite promises to maintain security of sensitive information, Eli Lilly inadvertently disclosed the names of consumers who used a prescription drug.

Our case against Microsoft illustrates that there can be law violations without a known or actual breach of security. Microsoft promised consumers that it would maintain a high level of security for its Passport and Passport Wallet system of accounts. Even though there was no actual security breach, after reviewing Microsoft's systems, the Commission alleged that Microsoft failed to take reasonably appropriate measures to maintain the security of consumers' personal information.

The case against Guess, Inc. illustrates that good security depends upon an ongoing process of risk assessment, identifying vulnerabilities, and taking reasonable steps to minimize or eliminate those risks. We alleged that Guess stored consumers' information, including credit card numbers, in clear unencrypted text, despite claims to the contrary.

Unencrypted information is vulnerable to attackers, something that is well known in the industry and can be corrected.

The Commission's settlements in these three cases require the companies to implement comprehensive information security programs. In addition, Microsoft and Guess must obtain an independent security audit every 2 years.

The Commission has engaged in a broad and continuing awareness and outreach campaign to educate businesses, consumers, and political leaders about the importance of cybersecurity. We work closely with industry, government agencies, and consumer groups to expand awareness. This is the single most essential element in creating a culture of security that is increasingly necessary for the protection of our critical infrastructure.

We have a first-class Web site focusing on safe computing practices. Our site provides a wealth of information on cybersecurity and how each of us can and must contribute to the effort. Our Web site registered more than 400,000 visits in the first year of deployment, making it one of the most popular FTC Web pages. And, a Google search recently indicates that 445 other Web sites link to our security site.

Every House and Senate office has a copy of our safe computing disk. And I might add, I will hold this up, and I think there is a package on your desk with a lot of our information security material in the package.

This CD disk was designed to assist each Member of Congress and staff in educating constituents on safe computing practices. Several Members of Congress have constructed excellent information security pages on their Web sites using information from the FTC. Each Member is an outstanding leader within his or her community and district. As the FTC's authorizing body and as the leaders in consumer protection, this committee in particular can partner with us effectively in our consumer awareness efforts on information security.

Our staff and I personally are standing by to help you and join with you in leading.

In addition to law enforcement and our awareness campaign, the Commission has taken an active leadership role in international efforts promoting cybersecurity. In 2002, the FTC led the U.S. Delegation, working with the OECD, to revise its security guidelines. The revised guidelines serve as an excellent, common sense start-

ing point for government, business, and organizations to implement information security. They address accountability, awareness, and action by all participants and form the basis for international cooperation toward establishing a culture of security. The guidelines have been embraced by the United Nations, APEC, nongovernment organizations, and many international businesses and associations.

In conclusion, attaining adequate information security will be a continuing journey; a long project, where complacency is not an option. I look forward to responding to your questions. Thank you.

[The prepared statement of Hon. Orson Swindle follows:]

PREPARED STATEMENT OF HON. ORSON SWINDEL, COMMISSIONER, FEDERAL TRADE COMMISSION

I. INTRODUCTION

Mr. Chairman, and members of the subcommittee, I am Commissioner Orson Swindle.[1] I appreciate the opportunity to appear before you today to discuss the Federal Trade Commission's role in protecting information security and its importance to both consumers and businesses.

Today, maintaining the security of our computer-driven information systems is essential to every aspect of our lives. A secure information infrastructure is required for the operation of everything from our traffic lights to our credit and financial systems, including our nuclear and electrical power supplies, and our emergency medical service. We are all, therefore, directly or indirectly linked together by this infrastructure. Consumers rely on and use computers at work and at home; increasingly, more consumers are making purchases over the Internet and paying bills and banking online.

These interconnected information systems provide enormous benefits to consumers, businesses, and government alike. At the same time, however, these systems can create serious vulnerabilities that threaten the security of the information stored and maintained in these systems as well as the continued viability of the systems themselves. Every day, security breaches cause real and tangible harms to businesses, other institutions, and consumers.[2] These breaches and the harm they do shake consumer confidence in the companies and systems to which they have entrusted their personal information.

II. THE FEDERAL TRADE COMMISSION'S ROLE

The Federal Trade Commission has a broad mandate to protect consumers and the Commission's approach to information security is similar to the approaches taken in our other consumer protection efforts. As such, the Commission has sought to address concerns about the security of our nation's computer systems through a combined approach that stresses the education of businesses, consumers, and government agencies about the fundamental importance of good security practices; law enforcement actions; and international cooperation. Our program encompasses efforts to ensure the security of computer networks, an understanding that we all have a role to play, as well as efforts to ensure that companies keep the promises they make to consumers about information security and privacy. In the information security matters, our enforcement tools derive from Section 5 of the FTC Act,[3] which prohibits unfair or deception acts or practices, and the Commission's Gramm-Leach-Bliley Safeguard Rule ("Safeguards Rule" or "Rule").[4] Our educational efforts include business education to promote compliance with the law, consumer and business education to help promote a "Culture of Security," international collaboration, public workshops to highlight emerging issues, and outreach to political leaders.

A. Section 5

The basic consumer protection statute enforced by the Commission is Section 5 of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[5] The statute defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[6] To date, the Commission's security cases have been based on deception,[7] which the Commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.[8]

The companies that have been subject to enforcement actions have made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. Their security measures, however, proved to be inadequate; their promises, therefore, deceptive.

Through the information security enforcement actions, the Commission has come to recognize several principles that govern any information security program.

1. Security procedures should be appropriate under the circumstances

First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures. It is highly problematic when a company inadvertently releases sensitive personal information due to inadequate security procedures.

The Commission's first information security case, Eli Lilly,[9] involved an alleged inadvertent disclosure of sensitive information despite the company's promises to maintain the security of that information. Specifically, Lilly put consumers' e-mail addresses in the "To" line of the e-mail that was sent to Prozac users who subscribed to a service on Lilly's website, essentially disclosing the identities of all of the Prozac user-subscribers.

Given the sensitivity of the information involved, this disclosure was a serious breach. Nevertheless, the Commission recognized that there is no such thing as "perfect" security and that breaches can occur even when a company has taken all reasonable precautions. Therefore, the Commission construed statements in Lilly's privacy policy as a promise to take steps "appropriate under the circumstances" to protect personal information. Similarly, the complaint alleged that the breach resulted from Lilly's "failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."[10] The focus was on the reasonableness of the company's efforts.

According to the complaint in the Lilly matter, the company failed, among other things, to provide appropriate training and oversight for the employee who sent the e-mail and to implement appropriate checks on the process of using sensitive customer data. The order contains strong relief that should provide significant protections for consumers, as well as "instructions" to companies. First, it prohibits the misrepresentations about the use of, and protection for, personal information. Second, it requires Lilly to implement a comprehensive information security program similar to the program required under the FTC's Gramm-Leach-Bliley Safeguards Rule, which is discussed below. Finally, to provide additional assurances that the information security program complies with the consent order, every year the company must have its program reviewed by a qualified person to ensure compliance.

2. Not All Security Breaches Are Violations of FTC Law

The second principle that arises from the Commission's enforcement in the information security area is that not all breaches of information security are violations of FTC law—the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen, as noted above, even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances.

When breaches occur, our staff reviews available information to determine whether the incident warrants further examination. If it does, the staff gathers information to enable us to assess the reasonableness of the company's procedures in light of the circumstances surrounding the breach. This allows the Commission to determine whether the breach resulted from the failure to have procedures in place that are reasonable in light of the sensitivity of the information. In many instances, we have concluded that FTC action is not warranted. When we find a failure to implement reasonable procedures, however, we act.

3. Law Violations Without a Known Breach of Security

The Commission's case against Microsoft[11] illustrates a third principle—that there can be law violations without a known breach of security. Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur before they take action. Particularly when explicit promises are made, companies have a legal obligation to take reasonable steps to guard against reasonably anticipated vulnerabilities.

Like Eli Lilly, Microsoft promised consumers that it would keep their information secure. Unlike Lilly, there was no specific security breach that triggered action by the Commission. The Commission's complaint alleged that there were significant security problems that, left uncorrected, could jeopardize the privacy of millions of consumers. In particular, the complaint alleged that Microsoft did not employ "suffi-

cient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained through Passport and Passport Wallet."[12] The complaint further alleged that Microsoft failed to have systems in place to prevent unauthorized access; detect unauthorized access; monitor for potential vulnerabilities; and record and retain systems information sufficient to perform security audits and investigations. Again, sensitive information was at issue—financial information including credit card numbers.

Like the Commission's order against Eli Lilly, the Microsoft order prohibits any misrepresentations about the use of, and protection for, personal information and requires Microsoft to implement a comprehensive information security program. In addition, Microsoft must have an independent professional certify, every two years, that the company's information security program meets or exceeds the standards in the order and is operating effectively.

4. Good Security is an Ongoing Process of Assessing Risks and Vulnerabilities

The Commission's third case, against Guess, Inc.,[13] highlighted a fourth principle—that good security is an ongoing process of assessing and addressing risks and vulnerabilities. The risks companies and consumers confront change over time. Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustments to reduce these risks.

The Guess case highlighted this crucial aspect of information security in the context of web-based applications and the databases associated with them. Databases frequently house sensitive data such as credit card numbers, and Web-based applications are often the "front door" to these databases. It is critical that online companies take reasonable steps to secure these aspects of their systems, especially when they have made promises about the security they provide for consumer information.

In Guess, the Commission alleged that the company broke such a promise concerning sensitive information collected through its website, www.guess.com. According to the Commission's complaint, by conducting a "web-based application" attack on the Guess website, an attacker gained access to a database containing 191,000 credit card numbers. This particular type of attack was well known in the industry and appeared on a variety of lists of known vulnerabilities. The complaint alleged that, despite specific claims that it provided security for the information collected from consumers through its website, Guess did not: employ commonly known, relatively low-cost methods to block web-application attacks; adopt policies and procedures to identify these and other vulnerabilities; or test its website and databases for known application vulnerabilities, which would have disclosed that the website and associated databases were at risk of attack. Essentially, the Commission alleged that the company had no system in place to test for known application vulnerabilities or to detect or to block attacks once they occurred.

In addition, the complaint alleged that Guess misrepresented that the personal information it obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times; but, in fact, after launching the attack, the attacker could read the personal information, including credit card numbers, stored on www.guess.com in clear, unencrypted text.

As in its prior security cases, the Commission's emphasis in Guess was on reasonableness. When the information is sensitive, the vulnerabilities well known, and the fixes inexpensive and relatively easy to implement, it is unreasonable simply to ignore the problem. As in the prior orders, the Commission's order against Guess prohibits the misrepresentations, requires Guess to implement a comprehensive information security program, and, like Microsoft, requires an independent audit every two years.

B. GLB Safeguards Rule

In addition to our enforcement authority under Section 5 of the FTC Act, the Commission also has responsibility for enforcing its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.[14] The Rule became effective on May 23 of this year, and the Commission expects that it will quickly become an important enforcement and guidance tool to ensure greater security for consumers' sensitive financial information. The Safeguards Rule requires a wide variety of financial institutions to implement comprehensive protections for customer information—many of them for the first time. If fully implemented by companies, as required, the Rule could go a long way to reduce risks to this information, including identity theft.

The Safeguards Rule requires financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of entities covered, the Rule requires a plan that accounts for each entity's particular circumstances—its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and management of system failures.

Prior to the Rule's effective date, the Commission issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements.[15] Commission staff also met, and continues to meet, with a variety of trade associations and companies to alert them to the Rule's requirements and to gain a better understanding of how the Rule is affecting particular industry segments. Now that the Rule is effective, the Commission is investigating compliance by covered entities.

C. Education and workshops

In addition to our law enforcement efforts and conducting outreach under the Commission's Safeguard's Rule, the Commission has engaged in a broad educational campaign to educate businesses and consumers about the importance of information security and the precautions they can take to protect or minimize risks to personal information. These efforts have included creation of an information security "mascot," Dewie the e-Turtle, who hosts a portion of the FTC website devoted to educating businesses and consumers about security,[16] publication of business guidance regarding common vulnerabilities in computer systems,[17] speeches by Commissioners and staff about the importance of this issue, and outreach to the international community. Many offices in the Commission including the Commission's Bureau of Consumer Protection, the Office of Public Affairs, and the Office of Congressional Relations, have participated in this effort to educate consumers and businesses.

The Commission's outreach effort is centered on the Commission's information security website.[18] The website registered more than 400,000 visits in its first year of deployment, making it one of the most popular FTC web pages. The site is now available in CD-ROM and PDF format and frequently updated with new information for consumers on cybersecurity issues. In addition, the Commission's Office of Consumer and Business Education has produced a video news release, which has been seen by an estimated 1.5 million consumers; distributed 160,000 postcards featuring Dewie and his information security message to approximately 400 college campuses nationwide; and coordinated the 2003 National Consumer Protection Week with a consortium of public- and private-sector organizations around the theme of information security.

Finally, the Commission's Office of Congressional Relations has conducted outreach through constituent service representatives in each of the 535 House and Senate member offices by mailing "Safe Computing" CDs. We would like to thank Chairman Stearns for his leadership on the issue of cybersecurity, and for encouraging his colleagues, in his July 18, 2003 "Dear Colleague" letter announcing the delivery of the FTC's safe Internet practices outreach kit, to educate their constituents on safe computing practices.

In addition, the Commission uses opportunities that arise in non-security cases to educate the public about security issues. For example, in early November, the Commission announced that a district court issued a temporary restraining order in an action against D Squared Solutions, and its principals.[19] The complaint alleged that the defendants operated a scam that barraged consumers' computers with repeated Windows Messenger Service pop up ads—most of which advertised software that consumers could purchase for about $25 to block future pop ups. Part of what made the defendants' conduct so egregious is that consumers continued to be bombarded by pop-ups, even when they were off of the Internet and working in other applications such as word-processing or spreadsheet programs and that the defendants allegedly either sold or licensed their pop-up sending-software to other people allowing them to engage in the conduct. The defendants' website allegedly

offered software that would allow buyers to send pop-ups to 135,000 Internet addresses per hour, along with a database of more than two billion unique addresses. Contrary to the defendants' representations, consumers, when educated about how the Windows operating systems works, can actually stop pop-up spam at no cost by changing the Windows default system.

In addition to bringing a law enforcement action to halt the defendants' conduct, the Commission issued an alert to consumers about the security issues raised in the case. The "Consumer Alert" provides instructions for consumers on how to disable the Windows Messenger Service in order to avoid other pop-up spam. The alert[20] also discusses the use of firewalls to block hackers from accessing consumers' computers.

Finally, the Commission continues, and will continue, to host workshops on information security issues when appropriate. Last summer, the Commission hosted two workshops focusing on the role technology plays in protecting personal information.[21] The first workshop focused on the technologies available to consumers to protect themselves. Panelists generally agreed that, to succeed in the marketplace, these technologies must be easy to use and built into the basic hardware and software consumers purchase.

The second workshop focused on the technologies available to businesses. We learned that businesses, like consumers, need technology that is easy to use and compatible with their other systems. Unfortunately, we also heard that too many technologies are sold before undergoing adequate testing and quality control, frustrating progress in this area.

The Commission also held a workshop on unsolicited commercial e-mail ("spam") which was instructive about the security risks that spam poses. We learned that, in addition to other problems, spam can also serve as a vehicle for malicious and damaging code.

D. International Efforts

In addition to our cases and domestic efforts, the Commission has taken an active international role in promoting cybersecurity. We recognize that American society and societies around the world need to think about security in a new way. The Internet and associated technology have literally made us a global community. We are joining with our neighbors in the global community in this enormous effort to educate and establish a culture of security.

During the summer of 2002, the Organization for Economic Cooperation and Development ("OECD") issued a set of principles for establishing a culture of security—principles that can assist us all in minimizing our vulnerabilities. Commissioner Swindle has had the opportunity to work with this organization and to head the U.S. Delegation to the Experts Group on the post-September 11 review of existing OECD Security Guidelines and to the Working Party on Information Security and Privacy.

The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."[22] The nine principles are an excellent, common-sense starting point for formulating a workable approach to security. They address awareness, accountability, and action. They also reflect the principles that guide the FTC in its analysis of security-related cases, including that security architecture and procedures should be appropriate for the kind of information collected and maintained and that good security is an ongoing process of assessing and addressing risks and vulnerabilities. These principles can be incorporated at all levels of use among consumers, government policy makers, and industry. They already have been the model for more sector-specific guidance by industry groups and associations.

Besides the OECD, the Commission also is involved in information privacy and cybersecurity work undertaken by the Asian Pacific Economic Cooperation ("APEC") forum. APEC's Council of Ministers endorsed the OECD Security Guidelines in 2002. Promoting information system and network security is one of its chief priorities. The APEC Electronic Commerce Steering Group ("ECSG") promotes awareness and responsibility for cybersecurity among small and medium-sized businesses that interact with consumers. Commission staff participated in APEC workshop and business education efforts this past year and is actively engaged in this work for the foreseeable future.

Along with the OECD and APEC, in December 2002, the United Nations General Assembly unanimously adopted a resolution calling for the creation of a global culture of cybersecurity. Other UN groups, international organizations, and bilateral groups with whom the Commission has dialogues, including the TransAtlantic Business and Consumer Dialogues, the Global Business Dialogue on Electronic Com-

merce, and bilateral governmental partners in Asia and in the EU also are working on cybersecurity initiatives.

Notwithstanding these global efforts, developing a "Culture of Security" is a daunting challenge. The FTC and other government agencies have a role to play, but the government cannot do this alone, nor should it try. The Commission is working with consumer groups, business, trade associations, and educators to instill this new way of thinking. We are encouraging our global partners to do the same and to share what is learned.

III. CONCLUSION

The Commission, through law enforcement and consumer and business education, is committed to reducing the harm that occurs through information security breaches. Maintaining good security practices is a critical step in preventing these breaches and the resulting harms, which can range from major nuisance to major destruction. The critical lesson in this information-based economy is that we are all in this together: government, private industry, and consumers, and we must all take appropriate steps to create a culture of security.

ENDNOTES

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any other Commissioner.

[2] For example, our recently released Identity Theft Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf, showed that over 27 million individuals have been victims of identity theft, which may have occurred either offline or online, in the last five years, including almost 10 million individuals in the last year alone. The survey also showed that the average loss to businesses was $4800 per victim. Although various laws limit consumers' liability for identity theft, their average loss was still $500—and much higher in certain circumstances.

[3] 15 U.S.C. § 45.

[4] 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[5] 15 U.S.C. § 45 (a) (1).

[6] 15 U.S.C. § 45(n).

[7] Where appropriate, the Commission has also brought Internet cases using the unfairness doctrine. See *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (Filed C.D. Cal. July 24 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

[8] Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.,* 103 F.T.C. 110, 174 (1984) (setting forth the commission's Deception Policy Statement.).

[9] The Commission's final decision and order against Eli Lilly is available at www.ftc.gov/os/2002/05/elilillydo.htm. The complaint is available at www.ftc.gov/os/2002/05/elilillycmp.htm.

[10] *Eli Lilly Complaint,* paragraph 7.

[11] The Commission's final decision and order against Microsoft is available at http://www.ftc.gov/os/2002/12/microsoftdecision.pdf. The complaint is available at http://www.ftc.gov/os/2002/12/microsoftcomplaint.pdf.

[12] *Microsoft Complaint,* paragraph 7.

[13] The Commission's final decision and order against Guess, Inc. is available at http://www.ftc.gov/os/2003/06/guessagree.htm. The complaint is available at http://www.ftc.gov/os/2003/06/guesscmp.htm.

[14] 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[15] Financial Institutions and Customer Data: *Complying with the Safeguards Rule,* available at http://www.ftc.gove/bcp/conline/pubs/buspubs/safeguards.htm.

[16] See http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html.

[17] See http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

[18] See http://www.ftc.gov/infosecurity.

[19] The Commission's press release announcing the case can be found at http://www.ftc.gov/opa/2003/11/dsquared.htm.

[20] The alert can be found at http://www.ftc.gov/bcp/conline/pubs/alerts/popalrt.html.

[21] Additional information about the workshops are available at http://www.ftc.gov/bcp/workshops/technology/indes.html.

[22] http://www.oecd.org/dataoecd/16/22/15582260.pdf

Mr. STEARNS. I thank the Commissioner.

Mr. Schmidt, welcome.

STATEMENT OF HOWARD A. SCHMIDT

Mr. SCHMIDT. Thank you, Mr. Chairman.

Chairman Stearns, distinguished members of the committee, my name is Howard Schmidt. I am the Vice President and Chief of Information Security for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring

so many global citizens together each day in this tremendous global marketplace.

I would like to thank you again for the opportunity to come before the committee for the second time and your continued leadership in this very important issue. Prior to arriving at eBay a few months ago, I had the privilege of being appointed by President Bush to lead, with Richard Clarke, the President's Critical Infrastructure Protection Board, which represented one part of the overall government response to the threat of cybersecurity attacks in the wake of September 11; and after 31 years retired, and we successfully published the National Strategy Defense for Cyberspace, working with a team of dedicated public servants, this body, and the American public.

In addition to my day job, I continue to proudly serve at the U.S. Army Reserves, assigned to the 701st MP Group as a Special Agent with the computer crimes section, and also serve on the board of directors for ISC Squared, the body that oversees certification for security professionals through the CISSB certification.

My remarks today will focus primarily on the changes that have taken place with both business and government to create the level of information-sharing and collaboration necessary to improve cybersecurity and to further improve security for consumers, as well as how the sharing and collaboration has indeed improved the level of information and protection of consumer data.

I would like to provide my update in specific examples of improvement in four major areas. Those areas are awareness and education, product enhancement, government activities and private sector initiatives. While these examples will not be comprehensive, they will indeed be some representative efforts we have undergone.

I would also state, even though my comments are very optimistic as where we have come from, I think we will also have a long way to go. I think under the block of awareness and education, one of the biggest visible changes that has taken place is the increase in dialog and training to better inform the end user and consumer on how to secure their computer systems and their information.

One of the first consumer-targeted awareness programs was truly a joint public/private partnership between many of the companies, the FTC, NSA, as well as some other government agencies, and it took place in the formation of the Cybersecurity Alliance, and the creation of our Web site, staysafeonline.info, which we drove out of the efforts of the White House. This Web site has a wealth of information to help even the most inexperienced users understand cybersecurity, potential threats from on-line criminals, and steps they can take to protect themselves.

In addition, we at the White House held a series of town hall meetings over the past 18 months to meet with private sector partners, individuals, parent-teacher organizations, with speakers ranging from CEOs of major financial institutions, to my distinguished colleague to my left, Commissioner Orson Swindle. Many of these town meetings were also Webcast to get the broadest audience to be able to see them and participate over the Internet.

Private sector companies have also held free seminars around the country, providing awareness to citizens. Many of these sessions focused on informing the elderly, one of the segments of our

society who has received great benefits in the on-line world and the resources that it can provide. Also, as we enter the holiday season, there will be mass media campaigns to educate consumers further on how to safely and securely enjoy the richness and robustness of the on-line e-commerce world.

Under product enhancements, another major improvement we have seen over the past 2 years has been the way security is now offered as a standard within software and hardware. One very visible example is with the hardware provided to use wireless technology and broadband, we now see firewalls being built directly into these components as well as antivirus software being built into wireless modem operations.

Major operating systems have now auto update features as antivirus functions. Many antivirus vendors have done an amazing job in speeding up the detection and analysis of many of the threats that you have mentioned in your opening comments of the viruses and trojans that are found in the wire. Many of them even provide free on-line services for consumers to be able to download and inspect their systems as a public service, and I noticed in the paper this morning, one of them is now offering free antivirus software for the next year.

Under the heading of government activities, there have been a number of great activities beyond the creation of the National Strategy to Defend Cyberspace. Recently the Department of Homeland Security created the U.S. Computer Emergency Response Team at Carnegie Mellon as a focal point for building partnerships based on cybersecurity response networks and providing a notification network of threats and vulnerabilities as they are discovered.

The Department of Justice, the U.S. Secret Service, and the FBI have significantly improved the response times and increased priorities around the investigation of cybercrimes. As a matter of fact, Director Mueller has placed cybercrime as one of the top five priorities within the FBI, and the Secret Service is growing a cadre of expert agents working with private sector called the Electronic Crime Task Force. Additionally, the Department of Defense continues to work in that area as well.

On the government effort, since these things have no borders, the State Department has done a wonderful job in creating multilateral and bilateral discussions with international partners, many of which the industry colleagues, some of us sitting here today, have been a part of since the very beginning.

Two quick examples in the private sector initiatives:

We know that there will be no silver bullets in enhancing cybersecurity, but recently we created a coalition to address specifically the area of on-line identity theft. We have fully recognized that the vast majority of identity theft occurs in the off-line world through dumpster diving and other mechanisms, but we have seen, as many of you have, an increase in criminals attempting to do the same thing on line.

The two recent methods are what we call phishing, with a p-h, or spoofed e-mails, where criminals send out thousands of e-mails telling people to update their information. We are working to address this in four areas: building new technologies to prevent this; second, to provide awareness and training to consumers so they are

better informed to not fall victim to these scams; third, to share information amongst very competitive companies on protection of these things; and fourth, to work with the law enforcement community to prevent these people through deterrence of investigation.

In closing, I want to cite three specific areas I think that we can look at because, despite the great security enhancements we have seen and will continue to see, there are clear challenges you must address.

We must review our commitment to enhance consumer awareness of basic cybersecurity practices, and the recent attacks have once again demonstrated how home users are now becoming the target.

Second, while we build an effective response network, we must not lose sight of the innovation frontier. Technologists on the horizon hold the potential to dramatically and potentially decisively transform our cybersecurity challenges. Self-healing computers, embedded technologies, can enable devices that recognize and defend against these attacks. We must not inhibit their ability to move forward in collaboration with our best universities.

And, finally, we must recognize that cybersecurity is no longer merely about product services and strategies. What is at stake in the effective implementation of advanced cybersecurity technology is nothing less than the ability to unleash the next wave of IT-led growth in jobs and productivity. Cybersecurity is an essential enabler.

In closing, I want to say that the next step of this will be on December 2 and 3. Homeland Security has invited a lot of the public service or private sector organizations to create a summit, creating a task force to move forward in a lot of those areas that we mentioned and we care very deeply about.

This concludes my prepared remarks and I thank you for the opportunity to be here.

[The prepared statement of Howard A. Schmidt follows:]

PREPARED STATEMENT OF HOWARD A. SCHMIDT, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, EBAY CORPORATION

INTRODUCTION

Chairman Stearns, distinguished members of the Committee, my name is Howard A. Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring so many global citizens together in this tremendous global marketplace each day. I would like to thank you for the opportunity to come before this Committee again as well as your continued leadership on this very important issue. Prior to my current position at eBay and subsequent to my last appearance, I had the privilege of being appointed by President Bush to lead, with Richard Clarke, the President's Critical Infrastructure Protection Board, which represented one part of the overall governmental response to the threat of cyber security attacks in the wake of September 11. I retired from 31 years of public service after completing and publishing the "National Strategy to Defend Cyberspace," working with a team of dedicated public servants, this body, and the American public.

I have had the privilege of working with committed individuals in the private sector, law enforcement, and government to forge the collaboration and cooperation that is so essential to safeguard cyber space for everyone, from inexperienced home users to large well-run corporate enterprises. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime in local law enforcement and the FBI. I also helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ISAC) and had the honor of serving as its first president.

I continue to proudly serve in the U.S. Army reserves, assigned to the 701st MP Group, (CID) as a Special Agent with the computer crime unit at CID headquarters. I also serve on the Board of Directors for ISC2, the body that oversees certification of security professionals through the CISSP certification. My remarks today will focus primarily on the changes that have taken place within both business and government to create the level of information sharing and collaboration necessary to improve Cybersecurity and further improve security for consumers, as well as how this sharing and collaboration has improved the level of information and protection of consumer computer data.

Today, the Internet connects over 170 million computers and an estimated 680 million users, with an estimated growth to 904 million by the end of 2004. From major data operations conducting large-scale financial transactions, to wireless devices keeping families connected, the Internet touches virtually all aspects of our economy and quality of life. eBay is a prime example of how deeply ingrained the Internet is in American life. Every day on eBay, millions of Americans, along with millions of people in countries around the world, come together to buy and sell all types of goods and services. Business relationships and, often, deep friendships are formed on the basis of commerce and shared interests. The eBay marketplace reflects the enormous power of the Internet to unite humanity at a crucial moment in history.

More pointedly, the Internet has become a fundamental component of business processes—enhancing productivity by speeding connectivity between remote locations or across functional operations. The Internet is deeply ingrained in managing power, producing chemicals, designing and manufacturing cars, managing money and delivering government services ranging from human services to environmental permitting. The flip side of these productivity-enhancing applications is an increase in attacks against the online community.

Today the Internet is utilized by hundreds of millions of users all across the globe sending information ranging from homework assignments and simple greetings to the most sensitive financial and operational data of government and industry, all at the speed of light. The Internet landscape also includes a private sector security industry that has grown to an estimated $17 billion per year in goods and services. And, as we are all painfully aware, attack speeds today are measured in seconds, not days.

I would like to provide my update in the format specific examples of improvement in four major areas. Those areas are: Awareness and education; product enhancements; government activities; and private sector initiatives. While we have made significant progress, I also want to stress that we still have much work to do and will continue to improve overall Cybersecurity by continued improvement in some of the examples I will mention today.

Awareness & Education:

One of the biggest visible changes that has taken place is increased dialogue and training to better inform the end user on how to secure their computers and information. One of the first consumer-targeted awareness programs was truly a joint private-public partnership. This partnership took place in the form of the Cyber Security Alliance. The alliance combined the expertise of a number of private sector entities with the efforts of government partners to create a comprehensive website for consumers. The website, www.staysafeonline.info has a wealth of information to help even the most inexperienced users understand cyber security, potential threats from online criminals, and steps they can take to protect themselves.

In addition, the White House held a series of town hall meetings around the country with private sector partners. These town hall meetings were open to the public and well-attended, with speakers ranging from CEOs of major financial institutions and exchanges, to subject-matter experts in cyber security. Many of these town hall meetings were webcast so those that could not attend in person could participate over the Internet.

Private sector companies have also held free seminars around the country to provide awareness to citizens. Many of the sessions focused on informing the elderly, one of the segments of our society that has received great benefit from the online world and the resources that it provides. As we enter the holiday shopping season, there will be mass media campaigns to educate consumers on how to safely and securely enjoy the richness and robustness of the online e-commerce world.

In the category of formal education, the National Security Agency (NSA) has a program identifying universities that meet the criteria to be designated a center of academic excellence in information security. This NSA program not only ensures the education of the next generation of information security professionals, but also guarantees that the university has sound cyber security practices in place as well as

awareness education for the students, who make up a large number of the online users and consumers. The NSA also administers the Cyber Corp program with NSF and OPM, providing scholarships for students in cyber security.

Product Enhancements:

Another major improvement that we have seen in the past two years is the way security enhancements are now offered standard in software and hardware. One very visible example is the hardware provided to use wireless technology. Broadband technology (Cable modem, DSL, satellites etc.) has given us capabilities and speeds that were only available to corporations before. We now see firewalls and the ability to download anti-virus software being built into wireless modems.

The major operating systems now have auto-update features included, and are now being turned on by default in more future versions. Products are now being shipped with many services turned off by default, thus making them more secure. Many of the online email services block potentially malicious code and do a much better job of blocking the Spam that often contains malicious functions.

Anti-virus vendors have done an amazing job in speeding up the detection, analysis and updates for many of the viruses that are found in the wild. Many of them even provide free online virus scans as a public service to assist consumers.

Government Activities:

There have been a number of government actions that have taken place since I last appeared before this committee—most notably the creation of the President's Critical Infrastructure Protection Board and the release of the National Strategy to Defend Cyberspace. This critical document set the framework for much of the private public partnerships, focusing a section on home users and small/medium enterprises.

I would also argue that the consolidation of cyber security related organizations into the Department of Homeland Security in the Infrastructure Protection Director was a valuable reorganization. The bringing together of the NIPC (FBI), Fed-CIRC (GSA), CIAO (Commerce), Energy Information Assurance Division (DoE) and the National Communications System (DoD) created a center of excellence that, with the help of focused leadership, will move to implement the national strategy. This new organization is called the National Cyber Security Division.

Recent action taken by the Department of Homeland Security (DHS) to create the US CERT at Carnegie Mellon University has the potential to significantly enhance security for all users. The US CERT is designed to serve as a focal point for building partnerships based cyber security response network and provide a notification network as threats and vulnerabilities are discovered.

The goal for US CERT is to ensure that there is an average response time of no less than 30 minutes in the case of any attack. The very specific nature of this goal is designed to deliberately focus the US CERT on building broad participation by the private sector.

The US CERT will undertake the following major initiatives:

- Develop common incident and vulnerability reporting protocols to accelerate information sharing across the public and private response communities;
- Develop initiatives to enhance and promote the development of response and warning technologies; and
- Forge partnerships to improve incident prevention methods and technologies;

The Dept. of Justice, the U.S. Secret Service and the FBI have significantly decreased their response times and increased priorities around investigations of cyber crimes. Director Mueller has placed cyber crime in the top 5 priorities at the FBI, and the Secret Service has added a number of electronic crime task forces in order to successfully investigate and prosecute cyber criminals. All of the Defense Department's investigative organizations have led the way investigating cyber crimes and have some of the best investigators in the world. The Department of Justice, through its Computer Crime and Intellectual Property Section, has chaired the G-8 Subcommittee on cyber crime and has been a significant driving force in combating worldwide cyber crime.

Since there are no borders when it comes to cyber space, and criminal attacks on consumers can come from all corners of the world, the State Department has conducted bilateral and multilateral discussions to ensure that there is international cooperation in the effort to protect cyber security.

I have had the extreme pleasure of working with Commissioner Swindel of the Federal Trade Commission, who has been a beacon of light for the protection of consumers' privacy and security. With his help in the creation of the FTC's "Dewey" program and his tireless support for town hall meetings, he truly has created a "culture of security" globally.

Private Sector Initiatives:

While there will be no silver bullets in enhancing cyber security, the private sector continues to grow its capabilities and make solid improvement in securing their part of cyberspace . Two of the earliest examples of private-public cooperation for "Cyber Crime/Cyber Security" were the the High Tech Crime Investigators Association (HTCIA) and the Information Systems Security Association (ISSA). Both organizations date back to the mid/late 80's and are dedicated to sharing nformation on cyber crime and information security. They still exist today and their membership and value have increased significantly over the years.

Most recently, the private sector has created a coalition that I see as an excellent example of efforts to enhance consumer cyber security. As you are probably aware, identity theft is a major problem. While the vast majority of ID theft occurs in the physical world, we have seen an increase in the activities of criminals to commit the same types of crime online. The most recent method is by using what we call "phishing" or "spoofed" emails. The criminals will send out thousands of emails telling people that there is an error with their online account and ask them to fill in an "update form" or their account will be closed. This form has the look and feel of major e-commerce sites—there was even a fake email from someone pretendingto be the FBI and asking unsuspecting users to enter personal information into a fake web site.

To combat this, many of the major players in the e-commerce space banded together to create an Anti-Online ID Theft Coalition. The Coalition boasts many private sector members, with the Information Technology Association of America providing support as the executive director. The Coalition has four major goals: 1) to build technology to reduce the likelihood of these mails even reaching their intended victim; 2) to provide awareness training to consumers so they can more readily identify these criminal acts; 3) to share information on new scams amongst the various security teams; and 4) to insure accountability by working with law enforcement to identify and prosecute these bad actors.

In a larger perspective, Sector Coordinators representing each of the major sectors of our economy have been appointed to fight potential cyber attack. A sector coordinator is an individual in the private sector identified by the sector lead agency to coordinate their sector, acting as an honest broker to organize and bring the sector together to work cooperatively on sector cyber security protection issues. The sector coordinator can be an individual or an institution from a private entity.

These private sector leaders provide the central conduit to the federal government for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures on a strategic level with regards to critical infrastructure protection activities. The sector coordinators and the various sector members were key to the creation of the National Strategy to Defend Cyber Space.

In addition, there has been a number of new private sector Information Sharing and Analysis Centers (ISACs). An ISAC is an operational mechanism to enable members to share information about vulnerabilities, threats, and incidents (cyber and physical). The sector coordinator develops these Centers with support from the sector liaison. In some cases, an ISAC Manager may be designated, who is responsible for the day-to-day operations of the ISAC, to work with the sector coordinator or the sector coordinating body with support from DHS and the lead federal agencies.

Despite these security enhancements, we can be certain that as increased collaboration continues to enhance our protection and responsiveness, the nature and sophistication of attacks will certainly evolve. There are clear challenges we must continue to address.

First, we must renew our commitment to enhance consumer awareness of basic cyber security practices. The recent attacks demonstrate that home users can be used as an effective pathway to launch attacks, or as a gateway into large enterprises. We need to build on the public/private initiatives to promote cyber security with a focused and aggressive outreach effort to benefit all consumers.

Second, while we build an effective response network we must not lose sight of the innovation frontier. Technologies on the horizon hold the potential to dramatically and potentially decisively transform our cyber security challenges. Self-healing computers, embedded technologies that enable devices to recognize and defend against attacks, and devices which enhance both security and privacy are within reach with an aggressive technology development agenda. This effort must be industry-led in collaboration with our best Universities. Most importantly, it must be synergistically linked with our response initiatives.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective

implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology-led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work, live, and learn.

I don't want to close without mentioning my expectation that many of these challenges will be addressed, and indeed met head-on, with tangible commitments and deliverables through the upcoming National Cyber Security Summit, to be held on December 2-3, 2003. This Summit will be co-hosted by the Information Technology Association of America, the U.S. Chamber of Commerce, TechNet and the Business Software Alliance, with the support of the Department of Homeland Security. I have the honor to serve at that summit, as will many of the brightest minds and most innovative companies across all sectors of the economy.

The work of this summit will continue past December 2-3 through task force work programs that will drive toward solutions in intense work before, during, and beyond the Summit. We expect that many of these proposals will be forwarded to DHS early next year, after which we can measure progress on an ongoing basis. We expect this to be an all-hands-on-deck effort where we bring together, distill, and integrate many of the outstanding work products from many groups regarding cyber security metrics, software development and maintenance, public outreach initiatives, and, of course, public-private partnerships in information sharing and early warning systems.

Chairman Stearns, this concludes my prepared remarks. I thank you for the opportunity to come before this Committee and welcome any questions that you and the Committee members may have.

Mr. STEARNS. Thank you.

Mr. Charney.

STATEMENT OF SCOTT CHARNEY

Mr. CHARNEY. Thank you. Chairman Stearns, Ranking Member Schakowsky, and members of the subcommittee, my name is Scott Charney, and I am Microsoft's Chief Trustworthy Computing Strategist.

I want to thank you for the opportunity to appear here today to provide our views on cybersecurity and what we are doing to secure consumer data. At Microsoft, security is our No. 1 priority. We are committed to continually improving the security of our software.

As Howard Schmidt just said, there are no silver bullets in cybersecurity; there will always be vulnerabilities in complex software and systems. As was true when we testified before you in 2001, cybersecurity involves many layers and many collaborative partnerships. In other words, cybersecurity involves management of technologies, as much as the technology itself.

Meanwhile, much has changed since we last testified before you. Consumer dependence on the Internet has grown. And as of March 2003, 30 million homes in America had a broadband connection to the Internet, double the number who had high-speed connections at the end of 2001.

Another key change over the past 2 years is that the time between the issuance of a patch and the time when we see a concrete exploit taking advantage of the underlying vulnerability has dramatically shortened. Therefore, once a patch is released, a race ensues between those installing the patch to eliminate the vulnerability and those developing code that exploits the vulnerability.

Moreover, the sophistication and severity of cyberattacks are also increasing. In response to these threats, industry has increased tremendously the resources and priority it devotes to cybersecurity issues, and the government has also taken significant steps during this time period to address these heightened risks for on-line con-

sumers, including creating the National Cybersecurity Division at the Department of Homeland Security and signing the Council of Europe's Cybercrime Treaty. We commend these actions as important steps and hope the Senate ratifies the treaty when it is received.

Security is Microsoft's top priority, and we know that security is a journey rather than a destination. 2 years ago before this committee, my friend and co-panelists Howard Schmidt properly stated: We know there is no finish line for these efforts, but by working as we have with industry peers and with governments, we have a chance to keep one step ahead of cyber criminals.

Shortly thereafter, Bill Gates had launched our trustworthy computing initiative, which involves every aspect of Microsoft and focuses on four key pillars: security, privacy, reliability, and business integrity. As part of this, we have enhanced the training of our developers to put security at the heart of software design and at the foundation of the development process.

Through this effort we are seeing a quantifiable decrease in vulnerabilities. For example, if you compare Windows Server 2000 and Windows Server 2003, for the last 6 months Windows Server 2003 has required fewer patches.

Another part of trustworthy computing involves communicating with our customers. In the wake of Blaster, we launched the Protect Your PC campaign, urging commerce to take three steps to improve their security, all available through Microsoft.com/protect.

Two years ago, we also spoke about the need of increased deterrence of criminal hacking. Although the Cybersecurity Enforcement Act passed last year, there is still much more that needs to be done. Despite the best and laudable efforts of dedicated law enforcement personnel, far too many hackers unleash their malicious code, commit crimes with no punishment. This is an untenable situation.

Earlier this month, we took a significant step to support law enforcement by creating the Antivirus Reward Program to provide monetary rewards for information resulting in the arrest and conviction of hackers. The government continues to play a key role in efforts to secure consumers' software and data.

I want to outline a few specific areas where government initiatives can be particularly helpful in promoting cybersecurity.

First, the public sector should increase its support for basic research and security technology.

Second, the government can lead by example by securing its own systems, buying software that is engineered for security, providing better training for government systems administrators and leading public awareness campaigns, such as the FTC's campaign featuring Dewey the Turtle.

Third, government and industry should reduce barriers to exchanges of information.

Fourth, law enforcement should receive additional resources. We also support the forfeiture of personal property used in committing these crimes.

Fifth, greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyberattacks.

In conclusion, we will continue to pursue trustworthy computing and to work closely with our partners in the computer software and communications industries, the government and our commerce to enhance cybersecurity.

Thank you, and I look forward to your questions.

[The prepared statement of Scott Charney follows:]

PREPARED STATEMENT OF SCOTT CHARNEY, CHIEF TRUSTWORTHY COMPUTING STRATEGIST, MICROSOFT CORPORATION

Chairman Stearns, Ranking Member Schakowsky, and Members of the Subcommittee: My name is Scott Charney, and I am Microsoft's Chief Trustworthy Computing Strategist. I want to thank you for the opportunity to appear today to provide our views on cybersecurity and on what we are doing to secure consumer data. I oversee the development of strategies to create more secure software and services and to enhance consumer security and privacy through our long-term Trustworthy Computing initiative. My goal is to reduce the number of successful computer attacks and increase the confidence of all computer users. This is something I have worked toward throughout much of my career, including during my service as chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division of the U.S. Department of Justice. While at CCIPS, I helped prosecute nearly every major hacker case in the United States from 1991 to 1999.

At Microsoft, security is our number one priority, and as an industry leader, we are committed to continually improving the capability of our software to protect the privacy of consumers and the security of their data. We are at the forefront of industry efforts to enhance the security of computer programs and networks and to educate consumers about good cybersecurity practices. We also work closely with our partners in industry and governments around the world to identify security threats to computer networks, share best practices, improve our coordinated responses to security breaches, and prevent computer attacks from happening in the first place.

This hearing is exceptionally timely because of the rapid developments in cybersecurity over the past two years. We wholeheartedly agree with this Subcommittee that it is critical for all of us to address consumer concerns about the privacy and security of their online data in order to stimulate the further growth of e-commerce and to help realize the Internet's full potential.

Today, I want to describe the risks posed to consumers' cybersecurity, and the ways in which industry and government are working together to protect consumers' online data. First, I will discuss the general state of cybersecurity since November 2001, when we last appeared before this Subcommittee; I will touch both on what has stayed the same, and on what has changed. Second, I will discuss Microsoft's ongoing efforts to help secure consumers' computer data. Third, I will offer a few suggested steps that the government can take to enhance the security of consumer data.

I. CYBERSECURITY SINCE NOVEMBER 2001

The pursuit of cybersecurity involves a daily and never-ending contest between industry, governments, and computer users, on the one hand, and cyber criminals, on the other. Hackers remain elusive, aggressive, and innovative. When we last testified before this Subcommittee on this topic, the "ILOVEYOU," Code Red, Ramen, Li0n, and Trinoo worms and viruses had already struck a variety of operating systems. Since that time, criminal hackers have unleashed Slapper, Scalper, Slammer, Blaster, SoBig, and many other viruses and worms to infect computers, deny service, and impair recovery.

There are no silver bullets in cybersecurity, and there will always be vulnerabilities in complex software and systems, as well as human errors made. As was true in 2001, cybersecurity involves many layers and many collaborative partnerships, including software design, software configuration, software patching, the sharing of threat and vulnerability information, user education, user practices, and the investigation and prosecution of cybercrime both within the United States and internationally. In other words, cybersecurity involves *management* of technology as much as the technology itself.

Meanwhile, much has changed since we last testified before you. Consumer dependence on the Internet has grown, and consumers are more frequently sharing their personal information, including their identities, contact information, financial data, and health information, over the Internet. Moreover, as the personal computer becomes more central to the daily lives of many citizens and to the daily functions

of the public and private sectors, the government, consumers, and business enterprises are storing more personal information on their Internet-connected computers and networks, thus potentially exposing their data to hackers even if that personal information is never transmitted over the Internet. In addition, consumers with broadband are, unlike those with a dial-up connection, connected to the Internet with unvarying IP addresses and at a high connection speed, and therefore place consumer data at greater risk. As of March 2003, 30 million homes in America had a broadband connection to the Internet, double the number who had a high-speed connection at home at the end of 2001 and a 50% increase from March 2002.

Another key change over the past two years is that the time between the issuance of a patch and the time when we see a concrete exploit taking advantage of the underlying vulnerability has dramatically shortened. This time period is crucial because we have had very few attacks that actually precede the patch; more typically, once a patch is released, a race ensues between those installing the patch to eliminate the vulnerability and those developing code that exploits the vulnerability. When an exploit is developed faster, enterprises and individuals have that much less time to learn of, test, and install the patch before a hacker uses the exploit to inflict damage. That window for the NIMDA virus was 331 days between patch release and exploit; for Blaster, less than two years later, it was only 26 days.

The chronology leading up to the criminal launch of the Blaster worm illustrates the complex interplay between software companies, security researchers, persons who publish exploit code, and hackers. On July 16, we delivered a patch for the vulnerability and a security bulletin to our customers. This was followed by ongoing outreach to consumers, analysts, the press, our industry partners, and the government. On July 25, nine days after we released the patch, a security research group called XFOCUS published a tool to exploit the vulnerability that the security bulletin and patch had highlighted. In essence, XFOCUS analyzed our patch by reverse engineering it to identify the vulnerability, then developed a means to attack the vulnerability, and finally offered that attack to the world so that any unsophisticated hacker could then unleash an attack by downloading XFOCUS's work and using launch tools freely available on the Internet.

At this point, we heightened our efforts to inform our customers about the steps they should take to secure their computers. On August 11, only 26 days after release of the patch, the Blaster worm was discovered as it spread through the Internet. This sequence of events underscores a dilemma: the same information that helps customers to secure their systems also enables self-identified security researchers and others to develop and publish exploit code, which hackers then use to launch damaging criminal attacks.

The sophistication and severity of cyberattacks are also increasing. The Slammer worm in January 2003 did not attack the data of infected systems, but resulted in a dramatic increase in network traffic worldwide and in temporary loss of Internet access for some users. This past summer, criminal hackers released the Blaster worm, which spread by exploiting a security vulnerability for which we had released a patch. Machines infected by Blaster used the network connection to locate new, vulnerable machines, whereupon the worm would copy itself, infect the new machine, and continue the process. Blaster affected Windows NT4, Windows XP, Windows 2000, and Windows Server 2003 systems, but could not reach those machines that were patched and defended by a properly configured firewall. The worm also tried to deny service to those users seeking to download the patch for Blaster.

In addition, cybercriminals have been able to make viruses more prevalent and harder for consumers to detect by "spoofing" legitimate email addresses, which makes it more difficult to determine who the real sender is. In 2002, there were twice as many email viruses as there were in 2001. In January 2003, the SoBig virus spoofed email addresses and contained infectious .pif attachments, which if opened would infect the user's computer and search the infected user's hard drive for email addresses of possible further victims. Multiple variants of the SoBig virus surfaced during the year. It is important to note that SoBig did not exploit any software vulnerability; it was a social engineering attack based on users' willingness to trust email that appeared to be from individuals whom they knew.

In response to these threats, industry has increased tremendously the resources and priority it devotes to cybersecurity issues. Many of those efforts continue today, and I will describe them in more detail in the next Section. Over the past two years, the government has also taken significant steps during this time period to address these heightened risks for online consumers. We commend these actions as important steps in our shared journey toward enhanced cybersecurity.

First and foremost, the Department of Homeland Security created the National Cyber Security Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate. The NCSD is established to provide 24 x 7

functions, including cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts. The Department created the NCSD as part of its implementation of the Homeland Security Act of 2002 and the *National Strategy to Secure Cyberspace,* which the White House released in February 2003 after soliciting extensive comments from consumers, industry, and other government actors. We worked with government officials in all of these activities, and we are encouraged by the work DHS has done to date. Moreover, I personally look forward to co-chairing a task force at its December "National Cyber Security Summit."

Second, the United States signed the Council of Europe Convention on Cybercrime in November 2001. The Convention requires parties to have minimum procedural tools to investigate such attacks, and to facilitate international cooperation in investigating those attacks. Because of the inherently international nature of cybercrime, the Council of Europe cybercrime treaty is an important step towards the transborder cooperation that is vital to combating cybercrime and protecting consumers. We look forward to the day when the treaty is sent to the Senate for its consideration.

II. OUR RESPONSE TO CYBERSECURITY THREATS TODAY

Security is Microsoft's top priority. We have devoted and will continue to devote enormous resources to enhancing security. As we confront new challenges and develop new approaches and new partnerships, we continue to learn that perfect security in cyberspace is unattainable, just as it is in the physical world. Operating system software is one of the most complex items that humans have created, and it is impossible to eliminate all software vulnerabilities. Thus, we know that security is a journey rather than a destination, and it can only be improved by partnerships involving government, industry, responsible security researchers, and customers around the world including government agencies, enterprises, and individual users. Two years ago before this committee, my friend and co-panelist Howard Schmidt properly stated, "We know that there is no finish line to these efforts, but by working as we have with industry peers—including some of these panelists—and with governments, we have a chance to keep one step ahead of cyber-criminals."

A. Trustworthy Computing

In January 2002, Bill Gates launched our Trustworthy Computing initiative, which involves every aspect of Microsoft and focuses on four key pillars: security, privacy, reliability, and business integrity. Security involves designing programs and systems that are resilient to attack so that the confidentiality, integrity, and availability of data and systems are protected. The goal of our privacy efforts is to give individual consumers greater control over their personal data and to ensure, as with the efforts against spam, their right to be left alone. Reliability means creating software and systems that are dependable, available when needed, and perform at expected levels. Finally business integrity means acting with honesty and integrity at all times, and engaging openly and transparently with customers.

Under the security pillar, we are working to create software and services for all of our customers that are Secure by Design, Secure by Default, and Secure in Deployment, and to communicate openly about our efforts.

- "Secure by Design" means two things: writing more secure code and architecting more secure software and services.
- "Secure by Default" means that computer software is more secure out of the box, with features turned off until needed and turned on by the users, whether it is in a home environment or an IT department.
- "Secure in Deployment" means making it easier for consumers, commercial and government users, and IT professionals to maintain the security of their systems.
- "Communications" means sharing what we learn both within and outside of Microsoft, providing clear channels for people to talk with us about security issues, and addressing those issues with governments, our industry counterparts, and the public.

The Trustworthy Computing goals are real and specific, and this effort is now ingrained in our culture and is part of the way we value our work.

We have enhanced the training of our developers to put security at the heart of software design and at the foundation of the development process. Security is and will continue to be our highest software development priority. All new software releases and service packs are now subject to an enhanced security release process which has already resulted in a notable decline of vulnerabilities in some of our server software. This effort, which can cost hundreds of millions of dollars and delay

the software's release to the market, is a critical step in improving software security and reliability. We are seeing a quantifiable and dramatic decrease in vulnerabilities: for example, Windows Server 2003 followed this process and in the first ninety days, we reported and patched three critical or important security vulnerabilities and six total in the first 180 days. Whereas in Windows Server 2000, we found eight critical or important vulnerabilities in the first ninety days, and twenty one in the first 180 days.

When an attack does occur, our Microsoft Security Response Center (MSRC) coordinates the investigation of reported vulnerabilities, the development of patches, and our customer outreach efforts. We are very proud of this organization and believe it represents the industry's state of the art response center.

Although we have made major strides, much work on Trustworthy Computing remains ahead of us. One key piece of that work is the Next-Generation Secure Computing Base (NGSCB). This is an on-going research and development effort to help create a safer computing environment for users by giving them access to four core hardware-based features missing in today's PCs: strong process isolation, sealed storage, a secure path to and from the user, and strong assurances of software identity. These changes, which require new PC hardware and software, can provide protection against malicious software and enhance user privacy, computer security, data protection and system integrity.

Part of Trustworthy Computing involves communicating with our customers. In the wake of Blaster, we launched the *Protect Your PC* campaign, urging customers to take three steps to improve their security: install and/or activate an Internet firewall, stay up to date on security patches, and install an anti-virus solution and keep it up to date. The www.microsoft.com/protect web site serves as the focal point for the campaign. We also provide a wide range of free security tools and prescriptive guidance to make it easier for consumers to make their computers and their data more secure.

B. Streamlining the Patching Process

Patch management is a significant issue. We recognize that the most important solution is to reduce the number of vulnerabilities in code, thus reducing the need for patching. This is why we are emphasizing secure by design. But no operating system—regardless of development model—will ever be free of all vulnerabilities. We must manage this risk by providing customers with simple and easy to use patches. To streamline those processes, we are taking the following steps:

- Improving our testing of patches to ensure patch quality.
- Reducing the number of patch installers to provide users with a consistent patch experience, and make patching simpler.
- Working to ensure that each patch is reversible, so a rollback is possible if deployment raises an unanticipated issue, such as adversely affecting a legacy application.
- Ensuring that patches register their presence on the system—and producing improved scanning tools—so a user can quickly determine if his or her machine is patched appropriately.
- Making our security patch releases more predictable. We are now providing security updates once a month, but we will still provide patches outside this schedule when necessary, such as when exploit code is publicly available.
- Avoiding reboot of the computer where practicable, as our customers are more likely to apply a patch more quickly, if server availability will not be interrupted.
- Producing specific technology, such as Software Update Services and Systems Management Server, so enterprises can download patches, test them in their unique environments, and then easily deploy them.
- Informing customers about the AutoUpdate feature in recent Microsoft operating systems, which can automatically download updates and then either install them as scheduled or request permission from the user to do so.

C. Securing Enterprises to Protect Consumers

As noted, protecting consumer security depends, in part, on protecting the security of enterprise servers, which often hold valuable consumer data. Steve Ballmer, Microsoft's Chief Executive Officer, announced last month that we are working to secure these networks from the hazards that arise when users log into those networks from home or other remote locations. Those hazards include malicious e-mails, viruses and worms, malicious web content, and buffer overruns.

While patches remain part of the solution, we are developing what we call safety technology to secure these networks at the perimeter by:

- Reducing the risk from computers such as notebooks and portable computers that are moved between an enterprise's network and external networks.
- Improving browsing technologies to minimize the risk of hostile web sites executing malicious code on visiting users' computers.
- Enhancing memory protection to help prevent successful buffer overrun attacks.
- Improving the Internet Connection Firewall within Windows while also working closely with partners in the software security industry.

Through these measures, we hope to help protect machines even when not patched, thus giving enterprises more time to test and deploy patches and enabling enterprises to patch on their schedule, not on a schedule determined by hackers.

We are also providing new information and guidance on how enterprises can secure their computers to protect data, including the personal information of their customers.

D. Industry Partnerships

We embrace our role in providing more secure computing for all our customers. Because security is an industry-wide issue, we participate actively in partnerships that span the industry, customers and both the public and private sectors to encourage customers to implement software in more secure ways.

For example, we are a founding member of the Organization for Internet Safety (OIS), an alliance of leading technology vendors, security researchers, and consultancies that is dedicated to the principle that security researchers and vendors should follow common processes and best practices to efficiently resolve security issues and to ensure that Internet users are protected.

We also work with the Virus Information Alliance (VIA), a centralized resource for Internet users seeking information about the latest virus threats. Through its member companies, Microsoft, Network Associates, Trend Micro, Computer Associates, Sybari, and Symantec, the VIA offers recommended best practices for preventing malicious attacks, information about specific viruses, how-to articles and links to other anti-virus resources on its web site.

I am personally participating with some of my co-panelists in the Global Council of Chief Security Officers, a newly formed think tank that will share information with member companies and governments on cybersecurity issues and enhance the involvement of private sector officials in cybersecurity issues.

We also helped found the Information Technology—Information Sharing and Analysis Center (IT—ISAC) and I serve on its board today. The IT-ISAC coordinates information-sharing on cyber-events among information technology companies and the government.

E. Anti-Virus Reward Program

Two years ago we spoke about the need to increase deterrence of criminal hacking. Although the Cyber Security Enforcement Act passed this Congress last year, there is still much more that needs to be done. Despite the best and laudable efforts of dedicated law enforcement personnel, far too many hackers unleash their malicious code or commit crimes with no punishment, as evidenced by the fact that the authorities have yet to bring to justice the criminals who launched major attacks like Blaster, NIMDA and Slammer. This is an untenable situation, and it is one the nation allows to persist in no other area. We need a robust deterrent to criminal activity online.

When criminal attacks are launched, we work with law enforcement officials to support their investigations. And earlier this month, we took a significant step to support them by creating the Anti-Virus Reward Program to provide monetary rewards for information resulting in the arrest and conviction of hackers. For example, we have announced a reward of $250,000 each for information leading to the arrest and conviction of those responsible for the SoBig virus and the Blaster worm.

To use a medical analogy, we are strengthening the Internet's immune system through initiatives such as the anti-virus reward program, our technical and legal anti-spam efforts, consumer education, and efforts to secure existing systems and to make security integral to new systems and applications. In the meantime, interim treatment will be necessary.

III. THE GOVERNMENT'S ROLE

The government continues to play a key role in efforts to secure consumers' software and data. We have recently collaborated with the Department of Homeland Security to raise awareness of cyberthreats through release of security bulletins. Such partnering between industry and the government is a vital step toward additional cybersecurity for consumers. I want to outline a few specific areas where government initiatives can be particularly helpful in promoting cybersecurity.

First, sustained public support of research and development continues to play a vital role in advancing the IT industry's efforts to secure consumers' software and data. A major portion of our $6.9 billion annual R&D investment goes to security, and accordingly, we support additional federal funding for basic cybersecurity research and development (R&D), including university-driven research. The public sector should increase its support for basic research in technology and should maintain its traditional support for transferring the results of federally-funded R&D under permissive licenses to the private sector so that all industry participants can further develop the technology and commercialize it to help make all software more secure.

Second, the government can lead by example by securing its own systems through the use of reasonable security practices, buying software that is engineered for security, and providing better training for government systems administrators. We also hope government will continue to promote security awareness among both home consumers and businesses—as the Federal Trade Commission did in its information campaign featuring Dewie the Turtle.

Third, government and industry should continue to examine and reduce barriers to appropriate exchanges of information, and to build mechanisms and interfaces for such exchanges. One encouraging step in this direction is the NCSD's recent creation of the National Computer Emergency Response Team (US-CERT). This coordination center, for the first time, links public and private response capabilities to facilitate communication of critical security information throughout the Internet community.

Fourth, it will take increased government commitment to root out those who hack into computers and propagate destructive worms and viruses that harm millions of computer users. Therefore, law enforcement should receive additional resources, personnel, and equipment in order to investigate and prosecute cyber crimes. We also support tough penalties on criminal hackers, such as forfeiture of personal property used in committing these crimes.

Fifth, because cybersecurity is inherently an international problem with international solutions, greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyber-attacks.

CONCLUSION

We will continue to pursue Trustworthy Computing and to work closely with our partners in the computer, software, and communications industries, the government, and our customers to enhance cybersecurity. In the end, a shared commitment to reducing cybersecurity risks and a coordinated response to cybersecurity threats of all kinds—one that is based on dialogue and cooperation between the public and private sectors—offer the greatest hope for protecting the privacy of consumer data, enhancing the confidence of consumers in the Internet, and fostering the growth of a vibrant, trustworthy online economy.

Mr. STEARNS. I thank the gentleman.

Mr. Morrow, welcome.

STATEMENT OF DAVID B. MORROW

Mr. MORROW. Thank you. Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify before you today on Cybersecurity and Consumer Data: What is at risk for the consumer?

My name is David Morrow and I am the Deputy Director of Global Security and Privacy Services at Electronic Data Systems, Incorporated. I have over 25 years of experience in the information technology field, with an emphasis on security. I am honored to join you today to present EDS's views on the state of information security or cybersecurity 2 years after my last appearance before the subcommittee.

I will focus today my comments on what has changed in the last 2 years, what needs improvement, and what can be done by both industry and the government to further protect our information networks. I will provide an outline here and request that my written comments be entered into the record.

So, what has changed? Thankfully, we have not seen another September 11. But as has been noted previously, we are still in a heightened threat environment. More recent attacks on our information networks, such as the DNS Root Server attacks in October 2002 and several high-profile virus and worm attacks, have not stopped us from relying on these networks to conduct business and live our lives.

In that context, here are some of the things that we are seeing: We are seeing an increase in the tempo and severity of new viruses and other attacks on our information infrastructure. That makes what we call "patch management" a much larger issue.

We are also seeing an alarming increase in the incidence of identity theft and criminal misuse of personal information that affects millions of Americans. Other changes are occurring in the regulatory environment. While regulations don't give detailed requirements for information security, and shouldn't in my opinion, they do have implications for improving the integrity of everyone's data. Due to the increasing number of attacks and some of the regulatory requirements, we are seeing an increased awareness of the problem. More clients are coming to us with questions about how to address their information and network security, but they are often still asking the wrong questions.

There is not one solution that can address everything. Information security is a continual process that elevates security planning out of the traditional information technology silo. Companies and agencies need to look at information security in a holistic way to create and integrate what has been dubbed "the culture of security" into their entire enterprise.

Despite this demonstrated critical importance and increased awareness, we have not seen a notable increase in the amount of investment that small and medium companies are making, and the government, are making in information security. There is cause for hope, however, because in a survey of corporate information officers released earlier this month by Forrester Research, increased funding for security and privacy efforts were at the top of the priority list for 2004.

What companies have been doing is committing some resources and expertise to the greater dialog in information security. Importantly, efforts are extending beyond the so-called high-technology sector into the greater business community, but more still needs to be done in that area.

EDS recently led a project in Business Roundtable to develop a cybersecurity road map for large corporations in any sector. "Building Security in the Digital Economy: An Executive Resource," was submitted as part of my written testimony.

So what needs improvement? Based on the changes I have mentioned, I would like to make two points about areas where we can do more. First, while I appreciate the increased level of awareness about information security, we need to improve on the level of real investment. In order to do that, we need to incorporate the notion of security as a business enabler into all of our business models. Enterprises that do so are investing in more strategic ways and are better able to serve their clients, consumers, citizens and business partners.

Second, we can improve upon the effectiveness of our information-sharing and public/private partnership efforts. We have made important strides in this area, but we need to do more to coordinate activities and results.

In sum, I would characterize that our state of information security information is marginally better than it was 2 years ago, with the hope for greater improvement.

So what can we do? I would like to make a few recommendations based on my comments today.

First, we can continue our efforts for a more coordinated program of industry/government cooperation.

Second, we can strive to improve information-sharing mechanisms and look for ways to collaborate across them as well as within them.

Third, we still believe that there are areas where incentives are necessary for companies to upgrade their information security, especially for small- and medium-sized companies. This is also particularly true for functions that the U.S. Government deems to be of critical importance to our economic and, therefore, our national security.

Fourth, we must continue to emphasize research and development for innovations in security.

Fifth, I still remain a strong proponent of ways in which we can develop and professionalize the cadre of information security professionals practicing today, including the expansion of programs beyond purely technical disciplines and into the more general business and general curriculums.

And finally, due to the interconnected networks that transcend traditional borders today, it is imperative that we engage in the overall global dialog on information security as well.

In conclusion, I would like to emphasize that the improvements we have made over the last 2 years in information security have much to do with increased awareness, and I support efforts such as this hearing toward that objective. We are now better off and we are leaning in the right direction, but we can and need to do more now. I outlined some suggestions for future focus that I hope are helpful.

Mr. Chairman, thank you for the opportunity to share my views and EDS's experience once again. I will be happy to answer questions you or members of the subcommittee may have.

[The prepared statement of David B. Morrow follows:]

PREPARED STATEMENT OF DAVID MORROW, DEPUTY DIRECTOR, GLOBAL SECURITY AND PRIVACY SERVICES, EDS

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to testify before you today on Cybersecurity and Consumer Data: What's at Risk for the Consumer. My name is David Morrow, and I am the deputy director for global security and privacy services at EDS. I have over 25 years of experience in the information technology ("IT") field as a computer programmer and analyst, operations chief, security officer, investigator, and consultant. Prior to joining EDS, I was a security consultant with Ernst and Young, LLP and Fiderus Strategic Security and Privacy Services, a small, start-up consulting firm. I also spent 13 years of a 22-year Air Force career as an investigator of computer crime for the Air Force Office of Special Investigations (AFOSI). When I retired in 1998, I was the Chief of the Computer Crime Investigations and Information Warfare Division for AFOSI. I am

honored to join you today to present EDS' views on the state of information technology security, two years after my last appearance before the Subcommittee.

In my testimony two years ago, I focused on the changes in our way of life after the tragedy of September 11, and the need to make investments to protect our information networks. I called upon government and industry to increase their collaboration, to focus not only on physical security but also information security, and to view cyber security as an essential capital investment rather than as an expense. I also noted a few ways that government can help industry bear the burden to protect our information economy and, therefore, our economic security. At the risk of repeating myself, I do want to emphasize that all those comments still hold true. Today, I will focus my comments on what has changed in the last two years, what needs improvement, and once again where I think both industry and government can make greater efforts.

What has changed?

Thankfully, we have not seen another September 11. However, we are still in a heightened threat environment. More recent attacks on our information networks, such as the DNS root server attacks in October 2002 and several high profile virus and worm attacks, have not stopped us from relying on them to conduct business and live our lives. In fact, we continue to look to information technology to drive innovation, efficiency, and productivity in our business operations. In addition, consumer use of the Internet for recreation and to conduct business continues to expand. And, our networks and the data on them are still vulnerable.

At EDS, we are seeing an increase in the tempo and severity of new viruses and other attacks on our information infrastructure. As I believe many of us predicted here two years ago, the complexity and sophistication of such attacks has continued to increase, making the task of defending and repairing our networks and systems all the more difficult. Installing software "patches" to deflect intrusions has become the favored way of addressing impending attacks. But, our clients are concerned about the need to install patch after patch after patch in rapid succession, on thousands of servers and tens of thousands of desktops. As you can imagine, it is a daunting task to do three major patch updates in one week in a large company or government agency. As these attacks become more frequent, severe, and sophisticated in often incompatible environments, what we call patch management has become a larger issue.

Unfortunately, another change we have seen is the increased incidence of identity theft and criminal misuse of personal information that affects millions of Americans at any given moment. While there are a variety of both high and low technology ways to obtain personal identity and credit information, the biggest "bang" for the criminal "buck" is still to locate and steal such information from an insecure network. I am disturbed by the increasing number of identity theft victims, and I believe more effective practices in network security and protection of personal data would benefit us all, both individually and as a society. I am glad to see that the Administration and Congress took the opportunity of reauthorizing the Fair Credit Reporting Act to address this challenge in a positive way and look forward to the passage of that legislation very soon.

Another change is the regulatory environment for us and for our clients. The Federal Trade Commission's new "Do-Not-Call-List", the Sarbanes-Oxley Act, and the pending FCRA reauthorization are the latest iterations. They follow the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. None of these regulatory frameworks give specific requirements for information security—and shouldn't, in my opinion. But in one way or another, either through greater corporate accountability, stronger privacy requirements, or new reporting obligations, each has direct or indirect implications for improving the integrity of data. As such, I would argue that each raises the level of awareness of information security in enterprises across the country.

This increasing awareness is a key component in the changes that I have seen in the last two years. More and more companies are coming to us with questions about how to address their information and network security. The problem is, they are still often asking the wrong questions. There is not a silver bullet that can address everything that achieves a stronger security posture. You can't point and click and say "done." There are no magic technologies or software. Information security is a continual process that elevates security planning out of the traditional information technology silo and involves the whole enterprise: IT, legal, regulatory, sales, marketing, and security, as well as each individual employee and business partner. It's hard work, but it's essential.

Another concern is the lack of details or guidance on standards of acceptable security practices. There are many organizations that are putting forth standards that

purport to drive best practices or interoperability, for example. But the proliferation of differing standards has caused some confusion among some of our clients that has prevented them from making important changes as they wait for further direction. We often use the ISO Standards because they are widely accepted, but there is room for improvement in developing standards for the future that are flexible enough to reflect changes in technology and business operations.

As modern global businesses become increasingly intertwined through partnerships, consortia, and merger and acquisition activity, traditional network and security boundaries are, in many cases, no longer intact. The security problems of one member of a partnership arrangement or newly acquired company now quickly become the problems of the entire group as the insecure network or system becomes the weak link in the entire chain. In addition, information security entails many things that may not appear to be security issues at first glance, such as enterprise training, for example. Addressing these issues requires strategic thinking about:

- the way a company or agency uses information, both on the network and off;
- what information is critical to the enterprise;
- what risk mitigation measures need to be put in place for what functions, how your information security fits into an overall business continuity plan; and
- how privacy and security policies and processes complement—or contradict—each other in the business.

Companies need to look at information security in a holistic way to create and integrate what has been dubbed a "culture of security" in to their enterprise. This may be a daunting task for those enterprises that are behind, but it is crucial to ensuring our economic security.

Despite its demonstrated critical importance, we have not seen a universally overwhelming increase in the amount of investment that companies or the government are making in information security. Some of the early adopters are often driven by regulation or in response to an attack, but there are many more who have taken a wait-and-see approach and hope that the next incident does not affect them—at least not too much. Part of that is a response to the current economic situation, and part is still a lack of understanding of the loss implications from an attack or even a natural disaster.

There is cause for hope, however. In a survey of corporate Chief Information Officers released earlier this month by Forrester Research, increased funding for security and privacy efforts were at the top of the list of priorities for 2004. I am hopeful that as the economy continues to recover, these plans will materialize into concrete actions and investment in the security and privacy of our national data resources.

What companies have been doing since September 11, is committing some resources and expertise to the greater dialogue on information security. Trade associations and other industry groups are including information security in their work program, or beefing up existing programs. New information sharing mechanisms are developing, existing ones are working to improve their impact, and industry groups are putting forth best practices and other guidance for their industry. EDS was a founding member of the Information Technology Information Sharing Analysis Center, or ISAC, one of 13 that were set up as part of Presidential Decision Directive 63 for the designated critical infrastructures. We have also taken on a role in the National Infrastructure Advisory Council (NIAC) that was established after September 11.

Importantly, efforts are also extending beyond the so-called high technology sector. EDS led an effort in the Business Roundtable, an association of Fortune 200 Chief Executive Officers, to develop a roadmap for large corporations in any sector to seriously consider their cyber security. The publication is called *Building Security in the Digital Economy: An Executive Resource* and is submitted as part of my written testimony.

What still needs improvement?

While I appreciate the increased level of awareness, I still think we need to do more to increase the level of real investment and improvement in information security. I believe it requires a recognition that security is not merely good for its own sake. We need to incorporate the notion of security as a business enabler into our business models. Enterprises that are looking at security as an enabler to their business are investing in more strategic ways, and are, therefore, better able to serve their clients, consumers, citizens, and business partners. As I said earlier, it's not just a business expense . . . it's an essential element in today's strategic—and networked—business model.

I believe the jury is still out on the role of the Department of Homeland Security in information security. We do applaud the creation of the National Cyber Security Division (NCSD) as well as its initial efforts on establishing the U.S. Computer

Emergency Response Team (US-CERT) and collaborating with industry. EDS will be participating in the Cyber Security Summit scheduled for early December and the ongoing work of the summit's designated task forces. However, we hope that its placement in the new agency does not illustrate a lack of concern, authority, or funding for information security efforts in the US government. We all need to be diligent to make sure the NCSD's efforts are maintained and relevant.

Virtually every one on this panel two years ago called for a public-private partnership and increased collaboration on cyber security. Arguably, we have made important strides in that direction as more companies, people, and agencies are talking about these issues in our associations and in government groups. These efforts are encouraging, but I argue we can do more, particularly by coordinating and learning from them, rather than duplicating them. In addition, once again we cannot look at individual aspects of security in isolation. As we consider our infrastructure protection, we have to look at the convergence of physical and cyber security because they can no longer be looked at independently.

In sum, I would characterize our state of information security readiness as marginally better than it was two years ago, with hope for greater improvement. While more are concerned, many are not doing as little as possible to remedy the problems they have. While more are aware of the threat, they are not mitigating the corresponding risks with appropriate measures. And, while there is more activity and public-private collaboration on information security, it is not well coordinated across the spectrum of industries and issues that are impacted by security measures.

What can be done?

First, we can continue our efforts for a more coordinated program of industry-government cooperation. The release of the Administration's *National Strategy to Secure Cyberspace* earlier this year provides a framework for continued work, and I urge both industry and government to take advantage of the upcoming Summit to solidify some of that work going forward. The Department of Homeland Security's National Cyber Security Division provides a focal point for monitoring industry efforts and participating as appropriate. As DHS solidifies its operations, we should ensure that the division has the appropriate mandate, funding, and industry coordination to support its activities.

Second, we can strive to improve information sharing mechanisms that are an important component of the public-private partnership on cyber security. For example, the Information Sharing and Analysis Centers (ISACs) are still active and are looking for ways to be more effective for their industries. I would argue the ISACs should also look for ways to communicate and even collaborate with each other when appropriate. Just as we cannot put information security into one silo, we cannot look at each industry sector in isolation. We are all interconnected now and rely on not only the security of our own network, but that of our suppliers, customers, partners, and competitors. Industry was collectively pleased when Congress provided for Freedom of Information Act exemptions for information shared on cyber security in the Homeland Security Act. We urge Congress to preserve the integrity of that provision in any future reviews of the Act in order to allow continued information sharing about vulnerabilities, breaches, attacks, and other actual or anticipated cyber incidents. Our experience has repeatedly shown that effective and timely information sharing is one of the most effective ways to prevent widespread incidents and to combat them when they do occur.

Third, we still believe there are areas where incentives are necessary for companies to allocate the necessary funds to upgrade their information security. This is particularly true for functions that the US Government deems to be of critical importance to our economic—and, therefore, our national security.

Fourth, we must continue to emphasize research and development for innovations in information security and encourage Congress to keep these avenues open for resolution in the budget process.

Fifth, I remain a strong proponent of ways in which we can continue to develop and professionalize the cadre of information security professionals practicing today. In the past two years we have seen a notable increase in the number of educational institutions offering courses and even advanced degrees in information security topics. While this is an encouraging sign, I still believe that there is great room for improvement in expanding the discussions beyond the purely technical disciplines and into the more general business curriculum.

Finally, as stated earlier, our intertwined information networks are global in nature and transcend traditional borders. That directly impacts global companies such as ours as well as consumers. It is imperative that we engage in the global dialogue on information security as well. I commend the Organization for Economic Coopera-

tion and Development and the Asia Pacific Economic Cooperation for their efforts to bring this issue to the international arena.

Conclusion

In conclusion, I would just like to emphasize the fact that the improvements we have made over that last two years in information security have much to do with an increasing awareness of cyber security concerns for all of us. Increased awareness here at home and abroad will continue to be crucial for our security going forward, and I support efforts such as this hearing toward that objective. We are better off and heading in the right direction, but we can and need to do more—now. I have outlined some suggestions for future focus that I hope are helpful to the Committee.

Mr. Chairman, thank you for the opportunity to share my views and EDS' experience once again. I will be happy to answer any questions you and the Members of the Subcommittee may have.

Mr. STEARNS. Thank you.

Ms. Davidson, welcome.

STATEMENT OF MARY ANN DAVIDSON

Ms. DAVIDSON. Thank you, Mr. Chairman, Ranking Member Schakowsky, and members of the subcommittee. My name is Mary Ann Davidson and I am the Chief Security Officer of Oracle. Thank you for inviting me here again to talk about the efforts information technology consumers, producers, caretakers, and policymakers can take to advance information assurance.

As you know, I appeared before the subcommittee just a few months after the events of September 11. In the shadow of one of the most tragic terrorist attacks in history, all of us contemplated the potential catastrophe caused by cyberterror on a massive scale.

While we have yet to witness a point-and-click terrorist attack, we have experienced, through Code Red, Blaster and SoBig, its forbears, billions of dollars in damage and lost productivity. These attacks are a grim reminder that far too much commercial software is built without attention to information assurance principles, leaving many of our national cyberassets vulnerable to attack; and the vulnerability increases every day.

Bounty money may nab us a few bad guys' scalps, but it won't slow the development of automated hacking tools. This is a cyber arms race and the bad guys are winning. For us at Oracle, the goal is clear: to achieve an industry culture where all commercial software is designed, developed, and deployed securely.

It has been said twice there are no silver bullets, so I won't say that. I will say it is not going to be a slam dunk. And, in fact, good intentions can do more harm than good. In California, a breach of a major data center prompted the legislature to hastily impose reporting requirements on security breaches. However well intended, the law was passed without a fundamental understanding of the limits of current technology and arguably could make the consumer data more vulnerable to unauthorized access.

We need sound ideas, not good intentions from government. Fortunately, the Federal Government can do good both as a software buyer and a policymaker to strengthen the culture of secure software.

The Federal Government first of all can leverage its buying power by insisting on more secure software. And we know at Oracle how this works, because we built security for 25 years, because of one of our important customer bases, who I affectionately refer as the "professional paranoids" asked us for it.

The Defense Department is setting an excellent example by enforcing a pro-security approach to procurement through NISSIP 11, which says for national security systems an agency can purchase only that software which has been independently evaluated under the Common Criteria or the Federal Information Processing Standards Cryptomodule Validation Program. That is a mouthful.

Since NSTISSP 11 went into effect 17 months ago, we have seen a number of positive developments. First, many firms are finally pursuing evaluations under FIPS of the Common Criteria for the first time, and it is high time.

Second, several firms, including Oracle, are financing evaluations of open-source products.

Third, many organizations, such as the financial services industry, are coming together to make security a purchasing criteria industrywide, and are using NSTISSP 11 as a model.

Thanks to NSTISSP 11, security is now far more in the software development consciousness than it was 2 years ago. That is a victory for which a large part of the credit goes to Congress and to DOD and the intelligence agencies.

There are other ways that the Federal Government can leverage its buying power. For example, the Federal Government could insist that the commercial software it buys is either defaulted to a secure setting "out of the box" or made easy for the customer to change security settings, such as through automated tools.

As more private and public consumers seek Common Criteria and FIPS as potential security benchmarks, a go-to clearinghouse is needed to validate vendor security claims and compare them to evaluation results themselves; to make apples-to-apples comparisons. For example, a couple of vendors can do common criteria evaluation and yet have far more stringent targets or less stringent targets. The clearinghouse would enable buyers to perform scorecarding and facilitate comparisons.

Evaluations can cost a half million dollars under the Common Criteria, so it is clearly not for everyone and probably not for consumer software. A software equivalent of the Underwriters Laboratories could ensure that even this kind of software is secure by design, delivering deployment.

Thanks to the UL, most consumer products are generally difficult to operate in an insecure fashion. We don't expect a consumer to do anything special to operate Cuisinarts securely; they just are secure. And, in fact, you have to make the product do something unnatural to hurt yourself while using it.

Consumers should not be expected to be computer security experts. Industry needs to make it easy for them to be secure.

Finally, a culture of security has to have an academic component for professional development and research in areas not addressed in the commercial marketplace. It is said, to err is human. A developer can check 20 of 21 conditions, and if failure to check the 21st causes a buffer overflow, the system is sometime vulnerable. Hackers only need to find one error, but developers have to close every one. It is an uneven battle. Federal support can help level the playing field.

Research is needed on tools that can scan software and pinpoint irregularities or back doors in the code. This type of product is not

seen as an attractive option among venture capitalists, because the dominant market mentality in information assurance is focused on developing a better Band-Aid, rather than an effective vaccine.

The recently enacted Cbersecurity Research and Development Act can be a useful resource for these types of challenges and Congress should make the highest possible investments to implement this legislation. If the medical community can eradicate smallpox with a strong investment in research, we should be able to eradicate buffer overflows. It is just code, after all.

The R&D Act can also fund new and improved academic programs and research centers on computer security in order to increase the number of graduates with this specialty. And, in fact, we need to change the mentality around who we allow to work on critical cyberinfrastructure. We don't allow engineers to design buildings merely because they use the coolest materials; they have to be licensed professional engineers.

A similar approach is needed in cybersecurity. Ignorance and hubris are the enemies of reliable cyberinfrastructure. Industry lacks for neither of these, unfortunately, so long as we hire based on knowledge of programming languages and not whether those employees understand the language of cybersecurity.

We are at war and all of our foot soldiers must be armed with the knowledge of what the enemy can and will do to the careless or unprepared. A strong academic component can also foster a diverse culture. Diversity will prevent the TI equivalent of the Irish potato famine, where reliance on one strain of potatoes brought on mass starvation and emigration.

Lack of biological diversity in many IT infrastructures has rendered them immensely susceptible to cyberplagues, and I daresay that far more than one-quarter of our population would be affected should the next cyberplague be more destructive than its predecessors.

Biological diversity breeds resistance and the lack of it is deadly.

Ultimately, any culture is as strong as the institutions it supported, so our hope is that government will work with us in an industry, in an academia to facilitate the institutions practices and mores necessary to build a vibrant strong culture and security. I believe we turned the corner and are making progress. We are extremely pleased to be a part of the next month's Cybersecurity Summit being planned by the Department of Homeland Security. That kind of dialog can ensure that we have turned the corner for the better.

Mr. STEARNS. I may need you to sum up.

Ms. DAVIDSON. Thank you, Mr. Chairman, and I thank you for the opportunity to appear before you today.

[The prepared statement of Mary Ann Davidson follows:]

PREPARED STATEMENT OF MARY ANN DAVIDSON, CHIEF SECURITY OFFICER, ORACLE CORPORATION

Mr. Chairman, Ranking Member Schakowsky, and members of the Subcommittee, my name is Mary Ann Davidson, Chief Security Officer of Oracle Corporation. Thank you for inviting me here again to talk about cybersecurity, and specifically, the efforts all of us can take—as information technology consumers, producers, caretakers and policymakers—to advance information assurance.

As you know, I appeared before this subcommittee just a few months after the ghastly events of September 11th. In the shadow of one of the most tragic terrorist

attacks in history, all of us contemplated the potential catastrophe caused by cyberterror on a massive scale, and the need for all of us to take far greater responsibility toward better information assurance.

While we have yet to witness a point-and-click terrorist attack, we have experienced, through CodeRed, Blaster and Sobig.F, its forebears, with billions of dollars in damage and lost productivity. These attacks are a grim reminder of what I warned this subcommittee two years ago: Far too much commercial software is built without attention to information assurance principles, leaving many of our national cyberassets—most in private hands—vulnerable to attack.

This vulnerability increases every day. Bounty money may result in the arrest of one or two of those responsible for cyberplagues, but it won't slow the development of advanced hacking tools, or change our increasing dependence on Internet-based platforms to administer public and private enterprises—two trends that are at the heart of our growing vulnerability. We are in our own version of an arms race, and the bad guys are winning.

For the information technology industry, our contribution to cybersecurity is straightforward: to achieve a marketplace and an industry culture where all commercial software is designed, delivered and deployed securely. There are no "silver bullets" to get there. A culture of security will require years to achieve and decades to maintain. Good intentions are not good enough and frankly, can do more harm than good. We already have seen one instance, in California, where a cyber-related event triggered a rush by the legislature to impose reporting requirements on security breaches. This law was passed without a fundamental understanding of the limits of current technology, and arguably could make consumer data more vulnerable to unauthorized access. It's not good intentions, but sound ideas that we need from government, and fortunately, there are a number of constructive steps the federal government can take, as both a software buyer and policy-maker to move us toward a culture of secure software.

Let the buyers be wary. Try as you might, Congress can't legislate good software. Those in a position to make a difference for the better are software consumers, from small business enterprises to big government agencies. All they have to do is make security a purchasing criterion. We at Oracle made the investments to integrate security throughout our development process because our customers asked for it. Our first customers, the intelligence community, who I affectionately call the "professional paranoids," are some of the most security-conscious people on the planet.

After ten years of an on-again, off-again merry-go-round by the federal government to become a more responsible software buyer, we are seeing constructive action being taken by the Defense Department to enforce a pro-security approach to software procurement known as NSTISSP #11. Simply put, for national security systems, an agency can only purchase commercial software that has been independently evaluated under the international Common Criteria (ISO 15408) or the Federal Information Processing Standards (FIPS) Cryptomodule Validation Program (CMVP).

Since NSTISSP #11 went into effect 14 months ago, we've seen several positive developments. First, a number of firms, including several of our competitors, are getting their products evaluated under FIPS or the Common Criteria for the first time. Second, we're seeing firms, including Oracle, financing evaluations of open source products. The security of open source versus proprietary software must not be a religious argument, as it so often is, but a business one. Open source, like proprietary software, is here to stay. We must all work to make it as secure as possible. Third, several industry organizations, such as the financial services industry, are coming together to make security a purchasing criterion industry-wide and are using NSTISSP #11 as a model.

We're seeing all of this because the initial impression from an industry perspective is that the federal government—the largest single buyer of commercial software—means business this time. As a result, security is now more in the software development consciousness than it was two years ago, and all of us as information technology consumers stand to benefit. That, in and of itself, is a major victory, and credit goes to the people within the Defense Department and intelligence agencies, as well as Congress, who are making a concerted effort to make this process work.

Secure "out of the box." NSTISSP #11 is a strong lesson that the federal government, acting as a security conscious software buyer, can change the entire commercial software landscape for the better. That said, are there ways, other than NSTISSP #11, that can accomplish the same purpose? We believe one measure worth considering is for the federal government to insist that the commercial software it buys is either defaulted to a secure setting right out of the box, or made easy for the customer to change security settings, for example, through automated tools that enable customers to become, and remain, secure. For example, the Office

of Management and Budget, working in conjunction with the federal agencies, the National Institute of Standards and Technology (NIST) and private industry, could specify what is the appropriate default security setting for the software it buys, or require appropriate and easy-to-use tools needed to change these settings.

Software Underwriters Lab. Government can be a useful vehicle to promote voluntary cooperation in the name of better security. For example, the Federal Trade Commission could work with the software industry to establish the software equivalent of the Underwriters Laboratories (UL). Security evaluations under the Common Criteria, which can cost half a million dollars per evaluation, are not for everyone, especially for many forms of consumer software. A software version of the UL is a cost-effective vehicle to capture less complex, more consumer-oriented forms of software. Again, the fundamental goal is to make all commercial software secure by design, delivery and deployment. To get there, the federal government should work with private industry to establish a consumer software equivalent of the UL. Thanks to the UL, most consumer products are generally difficult to operate in an insecure fashion. For example, Cuisinarts are designed so that you can't lose a finger while the blades are whirling. We don't expect the consumer to do anything special to operate Cuisinarts securely; they just are secure. Similarly, consumers should not be expected to be rocket scientists or security experts. Industry needs to make it easy to be secure.

Better Information for Buyers. There are already several good web sites to help private and public customers understand Common Criteria, FIPS and NSTISSP #11. However, particularly as more and more private customers see Common Criteria as a potential security benchmark, we are finding that what many of our customers need is a one stop, "go to" site in order to validate vendor security claims and compare them to the evaluation results themselves. It would be useful for a government procurement officer, or a private sector buyer, to be able to see all evaluations of any type, for a single vendor, at a single glance, from a single location, whether FIPS-140 or Common Criteria, whether evaluated here or abroad. This empowers them to make apples to apples comparisons. For example, two database vendors can both receive an EAL4 certification, even though one database vendor made two functionality claims in a security target, while the other database vendor made forty security claims. A clearinghouse would enable buyers to perform security target "scorecarding" and facilitate this and other types of comparisons.

Academic Research and Professional Development. As in many disciplines, the market alone cannot produce every security solution. A culture of security, like any professional culture, has to have an academic component for professional development, and to advance the field in areas not addressed in the commercial marketplace. For example, even with a good development process, "to err is human." A developer can check 20 of 21 conditions, and if failure to check the 21st causes a buffer overflow, the system is still potentially vulnerable. Keep in mind, hackers only need to find one error, while developers have to anticipate and close every one. It's an uneven battle. Federal government resources directed toward academic talent can work with industry and level the playing field.

One area that deserves attention, especially as more and more US firms partner with foreign countries on software development, is research on effective tools that can scan software and pinpoint irregularities or backdoors in the code. Unfortunately, this type of product research and development is not seen as an attractive option among venture capitalists, who generally channel their funds toward products that are nothing more than techno-band-aids for security faults. In other words, the market mentality toward information assurance is focused on developing a better Band-Aid, rather than an effective vaccine.

Congress last year took an important step in filling this void when it passed the Cyber Security Research and Development Act, which authorizes nearly a billion dollars over five years to invest in projects like code-scanning tools. We are about to enter the second year of this five-year program, and Congress is providing very limited assistance to pursue the goals of this legislation. We hope Congress will increase its investment.

If the medical community could eradicate smallpox with a strong investment in research, we should be able to eradicate buffer overflows. It's just code, after all.

A portion of the proposed investments under the Cyber Security R&D Act is authorized to create or improve academic programs and research centers on computer security in order to increase the number of graduates with this specialty. These kinds of investments are needed. The National Science Foundation reported earlier this year that only seven PhD's in cybersecurity are awarded each year. Research conducted more than two years ago found that while there were twenty-three schools identified as "centers of excellence" in information assurance, not one four-year university offered a bachelor's program in cybersecurity. Only one associate de-

gree program was offered at two-year institutions. We've seen some progress on this front, but much more can be done if the federal government invested more resources in this effort. The private sector can be a critical support component as well, especially given the current and growing demand for information security professionals among publicly held corporations.

In the IT industry, no one should be able to work on software that becomes part of critical infrastructure without proving that they understand and can demonstrate sound software design, coding and engineering principles. We do not allow engineers to design buildings merely because they use "the coolest materials." They must be licensed professional engineers. Why do we hire programmers to design critical IT infrastructure merely because they know the coolest programming languages? Ignorance and hubris are the enemies of reliable cyber infrastructure. Industry lacks for neither of these, unfortunately, so long as we hire based on what programming languages someone knows, and not whether they speak the language of cybersecurity. We are at war, and all our footsoldiers must be armed with the knowledge of what the enemy can and will do to the unprepared or careless.

A strong academic component in our culture of security also fosters a competitive and diverse culture. Strong competition and diversity will prevent the IT equivalent of the Irish potato famine, where reliance on one strain of potatoes brought on mass starvation and emigration. Similarly, lack of "biological" diversity in many IT infrastructures renders them immensely susceptible to cyberplagues. I dare say that far more than one quarter of our population would be affected should the next cyberplague be more destructive than its predecessors. Biological diversity breeds resistance. Lack of it is deadly.

As today's hackers and virus spreaders demonstrate every day, cybersecurity is an evolving discipline, one that combines art and science, and determination and passion. One cannot simply take a snapshot of a company's IT systems today and compare it to some preconceived list and say "yes, you are secure," or "yes, you are doing the right things toward better security." The state of the art is in a perpetual state of revolution.

Ultimately, any culture is as good as the institutions that serve as the foundation of that culture. So, if there is an overarching recommendation for you and your congressional colleagues, it is to work with us in industry and in academia to facilitate the development of the institutions, practices and mores necessary to build a strong, vibrant and diverse culture of security. I believe we have turned a corner, and are making progress toward getting more and more of our customers to think about security. Further steps are needed, such as the ones outlined here. Again, these recommendations are no silver bullets, but what we at Oracle believe are the next appropriate steps up this ladder of better security. We are very pleased to be a part of next month's Cybersecurity Summit being planned by the Department of Homeland Security, and some of our leading trade associations. Establishing that kind of regular, continuing dialogue is yet another link toward making sure we have truly turned a corner for the better, rather than yet another trip on the merry-go-round of information assurance.

Thank you again, Mr. Chairman, for the opportunity to appear before you today.

Mr. STEARNS. And I thank the gentlewoman.

Mr. Ansanelli.

STATEMENT OF JOSEPH G. ANSANELLI

Mr. ANSANELLI. Good morning. I am Joseph Ansanelli, CEO of Vontu. Our company provides information security software, specifically designed to help organizations protect consumer data by monitoring for the inappropriate distribution of non-public information via the Internet.

Mr. Chairman, members of the subcommittee, I commend your efforts in organizing this hearing.

The FTC recently provided, I think, an excellent answer for what is at risk for the consumer. As many of you know, in 2002 approximately 10,000,000 people were victims of identity theft. They reported $5 billion in out-of-pocket expenses and many hours repairing credit histories. In the last 5 years, almost 30 million people were victims. Clearly, identity theft is a risk for consumers. There is also a risk for businesses, who last year suffered an estimated

loss of nearly $48 billion. Additionally, businesses risk something even more important, the loss of consumer trust.

Vontu recently commissioned a study of 1,000 consumers to understand the relationship between consumer data security trust and commerce. Three highlights from this study. No. 1, security drives purchasing decisions. More than 75 percent of consumers said security and privacy were important in their purchasing decisions.

No. 2, consumer notification is important. About 80 percent of the consumers said that they wanted to be notified when companies are at least 75 percent sure that personal information has been compromised, and, three, all security violations are not the same. More than half of the respondents said they would be more concerned if their private information fell into the wrong hands due to an incident caused by an employee rather than a hacker.

This third point is very important. While most security testimony has focused on the remarks related to hackers breaking into computer networks from the outside, our focus is on the new security threat, insiders. Every day we create and store records that contain credit card numbers, Social Security numbers, and other types of non-public personal information. The sad fact is that many identity thieves never have to break into a firewall to get to this data. Their employer has already issued them the password to access this information. As a result, last year, a customer service representative of TeleData Communications who had easy access to consumer credit reports allegedly stole 30,000 customer records using his legitimate access. TeleData is the single largest identity theft crime ever prosecuted.

Also, the Secret Service has assembled teams to investigate fraud rings that enlist corporate employees to steal consumer information, and last consumer credit information provider Trans Union issued a report stating that the top cause of identity fraud today is now theft of records from employers or other businesses.

The problem with better protecting consumer data is no longer just an issue of keeping up with the hacker, but also one of ensuring that those with access keep the information secure. It is clear to me that we need new efforts to minimize this growing risk of identity theft as well as the insider threat.

However, I do not believe new government regulations alone can solve this problem. The right solution is a partnership with government and industry. To begin with, I suggest this committee consider developing a consumer data security standard, part of the Consumer Privacy Protection Act of 2003, H.R. 1636. This would ensure a nationally unified and standard approach to protecting consumer information. It should include a requirement for companies to do the basics in security, consider adding seat belts to automobiles. This requirement should include protecting and ensuring the confidentiality of non-public data, detecting potential misuse of consumer information, and correcting problems as they are discovered and notifying consumers when appropriate.

These requirements are similar to those under Gramm-Leach-Bliley and HIPAA. I ask you to consider if and why the industries covered by Gramm-Leach-Bliley and HIPAA are somehow unique in their need to protect the same personal data such as a credit

card and Social Security numbers that many other industries also store. It seems that any business it manages exposes consumers to identity theft risk and should be held to a similar standard.

Also, a national standard is important because confusion is the enemy of consumer protection. Unless a national standard emerges I fear that businesses will be forced to comply with a patchwork of 50 different State regulations.

Last, it is important to have a carrot to ensure partnership. The risk of civil lawsuits or steep fines discourages some companies from going beyond the basic requirement. We strongly suggest any future legislation include a regulatory carrot through a safe harbor to encourage companies to go beyond any basic security requirements without fear of severe penalties.

In closing, if not more is done to protect consumer information, especially in the electronic form, the cost of identity theft will continue to grow, causing a drag on this country to sustain its leading position in the global company.

I welcome the opportunity to answer any additional questions.

[The prepared statement of Joseph G. Ansanelli follows:]

PREPARED STATEMENT OF JOSEPH ANSANELLI, CHAIRMAN AND CEO OF VONTU, INC.

My name is Joseph Ansanelli and I am the CEO of Vontu, Inc. Our company provides information security software to help organizations protect consumer data by monitoring for the inappropriate distribution of non-public personal information via the internet. I am honored to provide testimony on information security, consumer data and the risks for consumers.

Identity Theft is the Risk for Consumers

The FTC recently provided an excellent answer to the question "What's at Risk for the Consumer?" They estimate that approximately 10 million people in the last year alone were victims of Identity Theft. These victims reported $5 billion in out-of-pocket expenses and countless hours of lost time repairing their credit histories. In the last five years, almost 30 million people or 10 percent of the US population were victims of identity theft. Clearly, identity theft is what is at risk for consumers.

Losing Consumer Trust is the Risk for Business

This is not only a risk for consumers, but is a risk for business as well. As part of the same FTC report, the losses to businesses totaled nearly $48 billion.

Additionally, there is a risk that is not mitigated through insurance or other strategies—loss of consumer trust. Vontu recently commissioned a survey of 1000 consumers in the United States to better understand the effect that security of customer data has on consumer trust and commerce. Some of the findings include:

- **Security drives purchasing decisions—**More than 75 percent of consumers said security and privacy were important in their decisions from whom they purchase.
- **Consumers will speak with their wallets—**Fifty percent said that they would move their business to another company if they did not have confidence in a company's ability to protect their personal data.
- **Insider theft increases concerns about a company's data security efforts—**More than 50 percent of the consumers surveyed said an insider breach would cause them to be more concerned about how a company secures their information

Clearly, financial costs and loss of consumer trust, as a result of identity theft, are what is at risk for business. The question is how does cybersecurity play into these risks?

The Insider—A Major Cause of Identity Theft

While most security testimony has focused on the threats related to hackers breaking into computer networks from the outside, my remarks today will focus a new and growing security threat—insiders. The sad fact is that many identity thieves never have to break through a firewall. Their employer has issued them a

username and password that gives them access to a virtual treasure trove of consumer data.

Everyday, companies throughout this country create and store millions of records that contain social security numbers, credit card numbers and other types of non-public personal information. At most of those companies, a significant percentage of employees have legitimate access to this data. This has created a potentially explosive combination of companies storing more consumer information and at the same time providing insiders with more access to that data.

Last year, the volatility of this combination made headlines. A customer service employee of Teledata Communications Inc. who had easy access to consumer credit reports allegedly stole 30,000 customer records. This theft caused millions of dollars in financial losses and demonstrates that even though any computer system can be hacked, it is much easier, and in many cases far more damaging, for information to be stolen from the inside.

Teledata is the single largest identity theft crime ever prosecuted. However, I am convinced that this kind of crime continues today, yet it often goes unrecognized. Insiders use their legitimate access to copy sensitive information and with a few clicks of their mouse, send it outside the company.

Law enforcement and regulators are also starting to raise the issue of the growing danger to consumers from insiders. Special Agent Tim Cadigan testified this summer that the Secret Service has assembled special teams to investigate the growing number of incidents where fraud rings enlist corporate employees in schemes to steal consumer information.

Mr. Howard Beales, Director of the Federal Trade Commission's Bureau of Consumer Protection, said in January that the FTC continues to see evidence that insiders were stealing consumer data at an increasing rate and using it to commit identity crimes. In September, the FTC reported that about a quarter of all consumers who knew that their information had been stolen believed that insiders were responsible.

Lastly, consumer credit information provider TransUnion recently issued a publicly available report stating that the top cause of identity fraud is now theft of records from employers or other businesses.

The problem of better protecting consumer data is no longer just an issue of keeping out the hacker but also one of ensuring that those with access to the data keep the information secure.

Consumer Data Security Standard

It is clear that we need new efforts to minimize this growing risk to consumers and businesses. However, I do not believe new government regulations alone can solve this problem. Instead, the right solution is to build a partnership of government and industry using both "the carrot and the stick".

To begin with, I suggest this committee develop a Consumer Data Security standard—possibly as part of the proposed Consumer Privacy Protection Act of 2003 (HR 1636). This standard would ensure a national, unified and standard approach to protecting consumer information and thereby stop one of the primary sources of identity theft. It should be self-regulating with oversight from appropriate agencies when problems arise and include a requirement for companies to:

- Protect and ensure the confidentiality of all non-public personal information;
- Detect potential misuse of consumer information;
- Ensure compliance by its workforce with their data security policies;
- Correct problems as they are discovered.

These requirements are similar to those required under Gramm Leach Bliley and HIPAA. Are the industries covered by these regulations unique in their need to protect personal data? It seems that any business that manages sensitive financial or other non-public personal information exposes consumers to identity theft. Whether it is providing your social security number when purchasing a mobile phone or using your credit card to buy groceries, you are exposing your personal information to theft—a cross-industry, unified approach is needed.

Additionally, this committee may want to make notification a part of this standard. In our survey, consumers said they wanted to be notified early and often when security and privacy violations occur. In fact, 80 percent said they want to be notified when companies are 75 percent sure that a violation has occurred.

This Consumer Data Security standard is the "stick" to ensure that there is a base level of responsibility for consumer data protection.

Safe Harbor

As mentioned earlier, a partnership between government and business is required to better protect consumer information. Unfortunately, today many of the current

and proposed Federal and State regulations serve as a disincentive to proactively search for insider breaches or inappropriate disclosures of consumer information. For example, the risk of civil lawsuits or regulatory censure discourages some companies from going beyond what is considered a base requirement. Future legislation should include a regulatory "carrot" through a "safe harbor" to encourage companies to go beyond basic security requirements and aggressively pursue potential leaks of data without fear of severe penalties.

This approach of the "carrot and stick" would not only encourage most companies to adopt new consumer protections quickly, it would free limited government resources to concentrate on the most egregious violations of the standard itself. Additionally, this proposal would help to solve one of the unaddressed issues regarding Identity Theft in both of the current Fair Credit Reporting Act bills approved this year by the House and the Senate.

In closing, the increasing costs of identity theft coupled with consumers' increased demands for security protection are driving these issues to the top of the agenda for consumers, business and government. If more is not done by all parties involved with respect to protecting electronic information, the costs will continue to grow, potentially affecting the country's ability to expand its leading position in the world economy.

I hope these comments will prove helpful to the subcommittee as it continues its deliberations on improving consumer data security. I welcome the opportunity to continue working with you, and am happy to answer any questions you might have.

Thank you.

Mr. STEARNS. Thank you.

Mr. Burton.

STATEMENT OF DANIEL BURTON

Mr. BURTON. Good morning, and thank you for the opportunity to testify.

My name is Dan Burton. I am Vice President of Government Affairs for Entrust, Inc., and as a world leader in securing digital identities and information, Entrust is driving the creation of a robust manageable business security environment through use of such technologies as encryption, digital signatures authentication and authorization.

I want to be very clear in my message. The cybersecurity problem is not getting better. Since 2001, when this subcommittee held a hearing on this issue, CERT reports a tripling of breaches from 52,000 to a projected 150,000 by the end of 2003. Although awareness has increased, understanding has not. Most companies are still struggling with this issue.

It is critical that this subcommittee provide the private sector with clear direction to protect sensitive consumer and business information. You can do so by strongly endorsing information and security governance programs that provide businesses risk assessment reporting and accountability. Let me give you some examples of the problem based on our market experience.

The first example speaks to the fact that even if you understand the threat, it is hard for companies to justify more than just a limited response because of the complexity and the investment in people, time and resources that is required. Last year, a large consumer data company suffered a breach when one of its customer's employees used the company's server to hack the passwords of other customers. This company believed that it had taken reasonable precautions to protect its data, especially since the penalties for not taking action were vague.

In this case, the seriousness of the breach and the new penalties created under California's SB 1386 forced the company to change

the way it thought about protecting its information systems. This company has put in place a much more robust set of security measures.

A second example speaks to the need to treat cybersecurity as a continuous process. A large financial institution implemented strong authentication digital signatures but year after year failed to upgrade its software, despite the fact that there was no cost to do so.

The reason? It did not have the systems in place to treat cybersecurity as a continuous process. Only when the company failed an audit and was cutoff from outside software support did senior management get involved and put in place the necessary procedures.

A final example shows how some companies are taking a more proactive approach. Several years ago, a major insurance company with a very large data base of confidential consumer records realized that it was a prime target for identity thieves and hackers. It couldn't simply lock up its records, since the field agents needed access to them, so it did a risk assessment and implemented a systemic information security governance plan. This program facilitated broad, highly secure access to data.

These three charges paint very different responses to the cybersecurity threat, but they all underscore a similar theme and one that I want to highlight today.

Companies need a clear understanding of cybersecurity costs, benefits, and penalties before they will make cybersecurity a priority.

Where do we stand? The growing array of Federal legislation does not go far enough to ensure companies take sufficient action. Some major laws affecting cybersecurity have been in place and have been referred to today, Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA. These laws tend to treat cybersecurity as a secondary issue. Two other cybersecurity laws are having a more immediate impact on market behavior, the California Breach Notification Act, SB 1386, and the Federal Information Security Management Act, FISMA.

Like it or not, and many people do not like it, by creating a private right of action for failure to report the breach of unencrypted personal information, SB 1386 has had a stark impact on industry's cost-benefit analysis and by treating cybersecurity as a management responsibility and tying it to OMB funding decisions, FISMA has had an immediate impact on the behavior of Federal agencies.

We think that there is an information security governance imperative. A governance's framework is important because it guides the implementation, evaluation and improvement of cybersecurity practices. A successful program requires three basic functions, risk assessment, reporting, accountability. It is our experience that in the absence of mandates for these activities, cybersecurity never receives the management attention and funding that are critical to succeed.

Entrust developed just such a framework for cybersecurity and brought it to the Business Software Alliance, which created a task force co-chaired by our CEO, Bill Conner. The BSA report released

last month entitled Information Security Governance Toward a Framework for Action highlights the fact that if we are to make real progress we must treat cybersecurity not only as a technical issue but as a management issue. We are also asked to co-chair the Governance Task Force at the upcoming DHS Cybersecurity Summit.

In conclusion, some compare cybersecurity to Y2K and emphasize the need to require public companies to report on their cybersecurity governance programs and their SEC filings. We didn't solve the Y2K problem by holding seminars for Cobol code writers. We solved it by engaging senior management in the issue and structuring liability laws appropriately.

Others have compared cybersecurity to on-line privacy and emphasize the need for voluntary reporting about risks, breaches and policies backed up by FTC enforcement. There is no privacy without security, and my favorite metaphor here is that of a canary in a glass cage in a room full of hungry cats. This canary has absolutely no privacy. However, it has perfect security. We have got to solve security first if in fact we want to have true on-line privacy.

Perhaps the best analogy for the issue, however, is quality. Like quality, cybersecurity requires numerous itegrative steps that are part of a continuous process. Companies must complete one cycle of the program, measure their progress, report their performance to senior management, fine-tune their efforts, and begin another cycle with slightly more rigor. Repeated cycles lead to improvements that will not only protect sensitive information but also enable productivity growth and new market opportunities.

As a global leader in the field with the benefit of firsthand knowledge and the best practices implemented around the world, Entrust strongly urges this subcommittee to lead the effort to take cybersecurity out of esoteric, technical discussions and into mainstream business management. The goal should be to encourage companies to treat cybersecurity as a corporate governance issue, which includes business risk assessment and reporting with management accountability. A good governance framework will produce a transparent process that includes executive management as responsible and assigns the——

Mr. STEARNS. Mr. Burton, I just need you to summarize.

Mr. BURTON. The cybersecurity is real, this is not a case of crying wolf. The statistics detail the increased damage and increased threats that occur daily. There is no reason to wait for a major breach or attack that incapacitates the Nation before acting, especially when there is strong consensus around of the steps industry must take. We are now all burdened with the awareness of the threat and have the corresponding responsibility to act. Congress must do everything that it can to ensure effective programs are in place for the private and government sector.

Thank you.

[The prepared statement of Daniel Burton follows:]

PREPARED STATEMENT OF DANIEL BURTON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, ENTRUST, INC.

Good Morning. Chairman Stearns and Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject. My name is Daniel Burton, and I am Vice President of Government Affairs for Entrust,

Inc. In my testimony today, I will address our view of where the private sector stands in its efforts to secure its information systems and what this Subcommittee can do to accelerate progress.

I want to be very clear in my message. The cyber security problem is not getting better. Since 2001, when this committee held a hearing on this issue, CERT has reported a tripling of cyber security breaches, from 52,000 in 2001 to a projected 150,000 by the end of 2003. Although some companies have recognized the threat of cyber attacks to their business performance and their customers' personal information, most are struggling to deal with the issue. It is incumbent on this Subcommittee to galvanize industry efforts to protect sensitive consumer and business information. This can only be accomplished by securing the private sector IT systems that control the majority of the nation's critical infrastructure. You can do so by strongly endorsing information security governance programs that drive business risk assessment, reporting and accountability.

Entrust is a world leader in securing digital identities and information. Over 1,200 enterprises and government agencies in more than 50 countries use our security software solutions, so we have a good perspective on today's cyber security reality. As a company, we are leading the evolution from defensive, perimeter-oriented technology approaches to a more proactive business security strategy that enables increased productivity. This strategy involves creating a more robust, manageable business security environment through the use of technologies such as encryption, digital signatures, authentication and authorization. We also work with customers to put in place the policies and procedures that protect digital identities and information. Our biggest competition comes not from other companies, but from the "do nothing" business mindset regarding cyber security.

I. EXAMPLES OF THE PROBLEM

A few examples based on Entrust's experience in the market show how enterprises are responding to cyber security today.

Last year, a company that is a large collector and processor of consumer data suffered a breach when one of its customer's employees used the company's servers to hack the passwords of its other customers. The hacker then proceeded to access and copy databases containing highly personal consumer information. Because this company's clients include 14 of the top 15 credit card companies, 7 of the top ten automakers and 5 of the top 6 retail banks, in addition to other major consumer brands, the attack was not a trivial hack. Fortunately, no identity theft complaints have been traced directly to this breach. Despite the fact that many people focus on external threats, it is important to note that this breach, like most, was internal, meaning that it came from an insider. Moreover, it was discovered only by accident ten months after the incident occurred when law enforcement agents researching another breach discovered e-mails describing this one. As soon as the company learned of the attack, it informed its customers, as required by the California cyber security breach notification law (SB 1386), and implemented authentication and encryption systems to better protect its data.

As a major database company with a pretty good security and privacy program, this company believed that it had taken reasonable precautions to protect its data, especially since it was doing as much as many other companies and the penalties for not taking action are vague. In this respect, it is typical of many companies. The reality facing business today is that even if you understand the threat, it is hard to justify more than limited cyber security measures because of the complexity involved and the investment in people, time and resources that is required. In this case, however, the seriousness of the breach and the new penalties created under California SB 1386 forced the company to change the way it thought about protecting its information systems. Today, this company is on the forefront of driving a higher standard and better understanding of cyber security reality.

A second example speaks to the need to treat cyber security as a continuous process. Several years ago, a large financial institution implemented strong authentication and digital signatures on its cash management service offering for its business customers. I should note that billions of dollars traverse this network. Although there was no additional fee to upgrade this technology as new versions of the software were released, the company repeatedly failed to do so. The reason? It did not have the systems in place to treat cyber security as a continuous process. Only when the company failed an audit because it was cut off from software support did senior management become involved and take the necessary steps to upgrade the company's security systems.

A third example shows that, despite the lip service they pay to the issue, some companies are unwilling to do anything about cyber security that will affect applica-

tion performance. A major investment bank realized that it did not have adequate cyber security protections in place and undertook a review of solutions to securely authenticate its sensitive communications internally and with customers. As a condition of this review, however, it stated that it was not willing to sacrifice any application performance for better security. This meant that it would accept only a few milliseconds response time for authentication during fail over. Since no security products can meet this standard, now the company is deciding whether they will tolerate even a minimal performance compromise in order to include security.

A fourth example involves Federal agencies, which in their size and complexity are similar to large enterprises. Until a few years ago, the Federal government did not have an adequate cyber security policy, despite the fact that year after year Congressional report cards gave most government agencies an "F" in information security. It was not until Congress passed the Government Information Security Reform Act (GISRA), later amended by the Federal Information Management Security Act (FISMA)—which coupled IT security performance with OMB budget controls—that Federal agencies began to change. By insisting that cyber security be treated as a governance and budget issue with risk assessment, reporting and senior management engagement, FISMA and OMB forced Federal agencies to begin to upgrade their cyber security programs.

A final example shows that when companies view cyber security as a business enabler that improves productivity, they are more likely to be proactive. Several years ago, a major insurance company with a large database of confidential customer records realized that it was a prime target for identity thieves and hackers. The insurance company couldn't simply lock up its records since it had thousands of field agents that needed to access them to service customer needs. In order to solve this problem, the insurance company did a comprehensive risk assessment and, using digital signatures and authentication technology, implemented an information security governance plan that encompassed strategy, technology, people and process. By proactively securing its IT systems, the company not only protected confidential customer information, but also created the secure business operations necessary to increase the productivity of its agents.

Although these examples paint different responses to the cyber security threat, they all underscore a similar theme—without a better business understanding of cyber security costs, benefits and penalties, most companies will take only limited cyber security measures.

II. WHERE DO WE STAND?

Regardless of how you grade industry's response, there is no doubt that the cyber security risk is increasing. Although some companies are responding, overall business progress has been slow. The current situation brings to mind the "boiling frog" metaphor. If you drop a frog in boiling water, it will jump out. However, if you put a frog in a pot of water and gradually raise the temperature, the frog will cook. I think many companies are being "cooked" when it comes to cyber security.

Like quality improvement, cyber security is not a one-time event, but a continuous process. Just as few managers understood the quality movement when Deming first introduced it, few business leaders fully grasp the new and evolving discipline of cyber security today. We are at the beginning of this brave new digital frontier, and Congress must find ways to accelerate industry's understanding and progress. Companies make little distinction between cyber terrorism, cyber crime and cyber vandalism. The fact that different actors with different motives perpetrate these attacks may be significant to government enforcement agencies, but it is of little consequence to industry. As far as industry is concerned, the primary question is not, who was responsible for the attack? But, how much damage did it cause? What is the likelihood that it will happen again? And, what are the cost, liability and brand implications? Anything that Congress can do to bring incentives for constructive action and clarity to industry's assessment of costs and benefits will help in the effort to protect our critical infrastructure.

The growing array of Federal legislation has not adequately addressed this issue. Some major laws affecting cyber security are already in place, such as the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. These laws, however, tend to treat cyber security as a secondary issue and cite requirements that are often so vague that they do little to improve focus or understanding of the issue or help industry better calculate costs and benefits. Faced with weighing ambiguous cyber security risks against other business and economic realities, companies have tended to follow one of three paths. Some have chosen to do nothing and wait until either the threat becomes more potent or regulatory requirements get clarified. Others—probably the majority—have made some

initial efforts, but have not really integrated cyber security into their core business operations. A third group—comprised of only a rare few exceptions—has embraced cyber security as a market differentiator, integrating it into their core operations and elevating it to an executive management concern.

Two other cyber security laws, however, are having a more immediate and profound effect on market behavior: the California cyber security breach notification act (SB 1386) and the Federal Information Security Management Act (FISMA). These laws are specific about cyber security penalties and programs. By creating private rights of action and penalties for failure to report breaches of unencrypted personal information, SB 1386 has changed industry's cost-benefit analysis. And by treating cyber security as management responsibility that entails risk assessment and reporting, the Federal Information Security Management Act outlined a roadmap for Federal agencies that has enabled progress.

III. THE INFORMATION SECURITY GOVERNANCE IMPERATIVE

Given the increased awareness of the problem, the lack of understanding, and the legislative ambiguity, Entrust has moved proactively to foster collaboration between the public and private sectors on this topic. We first began working this issue inside our company, with the active engagement of our Board of Directors and executive management. At the direction of our CEO, Entrust began to develop and implement just such a cyber security governance program last year. As an information security software company, we felt it was our responsibility to help create a framework that would allow for appropriate risk assessments, performance measures, management guidelines and board audits. The program we developed is tailored to the business needs of Entrust and embodies our interpretation of ISO/IEC 17799 and how the Federal Information Management Act (FISMA) can be applied to the private sector. We identified 141 elements that were important to measure progress. When we started, 25 of these elements were in the red, indicating the need for serious improvement; today, only two are. Our journey is off and running but not over.

As an information security software company who lives in this space, our experience raises real concerns about the status of the average company and the country. As we discovered at the starting point of our cyber security review, we were not nearly as secure as we would have predicted. This discovery made us wonder whether other companies are are making real and "measurable" progress since many of them lack a framework.

As a result of our experience, Entrust brought this framework to the Business Software Alliance (BSA) who created a cyber security task force co-chaired by Entrust's CEO, Bill Conner. The BSA report, entitled, *Information Security Governance: Toward a Framework for Action,* released in October 2003, found that information security is not only a technical issue, but also a corporate governance challenge. To quote that report,

> *While there is broad consensus on the actions needed to create strong security, too often responsibility is left to the chief information officer or the chief information security officer. In fact, strong security requires the active engagement of executive management. By treating these challenges as a governance issue and defining specific tasks that employees at all levels of an organization can discharge, enterprises can begin to create a management framework that will lead to positive results.*

A governance framework is important because it guides the implementation, evaluation and improvement of cyber security practices. An organization that creates such a framework can use it to articulate goals and responsibilities and evaluate progress over time. One of the most important aspects of such a framework is that by defining business and cyber security responsibilities within an organization, it creates a roadmap for improvement. By specifying who does what and forcing companies to report on their results to their own boards, it allows companies to assign specific responsibilities and translate awareness into action.

Effective cyber security governance programs usually have three basic functions: risk assessment, reporting and accountability. Their payoff comes from the fact that they insist on the systematic oversight and execution necessary to make cyber security part of a company's core business operations. Simply identifying best practices is not enough; they must be married with effective implementation at all levels of an organization. To be effective, each information security program must be tailored to the needs of the individual business and industry in which it operates. It must identify business drivers; clarify roles and responsibilities; recognize commonalities; define metrics; include periodic progress reports to executive management; and specify what corporate executives, business unit heads, senior managers, and CIOs should do.

According to the BSA information security governance report, the board and the CEO has responsibility for overseeing policy coordination, business unit compliance and accountability. The business unit head has responsibility for providing information security protection commensurate with the company's risks and business needs, as well as training, controls, and reporting. The senior manager has responsibility for securing information and systems, assessing assets, determining appropriate levels of security, cost-effectively reducing risk, testing and controls. The CIO and CISO have responsibility for developing and maintaining compliance with the security program, designating a security officer, developing the required policies, assisting senior managers, and conducting a security awareness program.

IV. CONCLUSION

Congress should embrace requirements for information security governance and reporting. Citing the Y2K experience, some have emphasized the need for a ruling that would require public companies to report on cyber security governance programs in their SEC filings. In order for such a provision to be successful, it will be necessary to avoid esoteric requirements that increase the cost and complexity of implementing solutions but do little to increase cyber security and shareholder value. Others have cited the online privacy debate and emphasized the need for voluntary reporting about cyber security policies and breaches, backed up by FTC enforcement. For this approach to succeed, it must also encompass the need to secure business information systems. Still others have compared cyber security to the quality movement and insisted that government provide incentives for companies to undertake the training and process improvements necessary to secure their information systems.

We would recommend the following lessons for companies intent on securing our critical infrastructure:

- A business information security governance framework for risk assessment and reporting with executive management engagement and board oversight is essential. A good governance framework will produce a transparent process that allows management to assign responsibility and make investment decisions to address unacceptable risks.
- Businesses need to get on with it—just do it. Information security is a very broad topic with seemingly endless detail. Companies should not try to solve the problem all at once. Instead, they should begin with the top-level policy issues. The important thing is to get started. Too many programs never get off the ground because the effort looks too daunting.
- Business information security governance is a continuous improvement program. Like quality, cyber security improvement requires numerous iterative exercises in a continuous journey. Companies should complete one cycle of the program at a high level, report to the Board on their performance, fine-tune their program and begin another cycle with slightly more rigor. Repeated cycles will lead to real improvements.

Whatever course is taken, the objective should be to encourage companies to treat cyber security as a corporate governance issue that includes business risk assessment and reporting with management accountability. The cyber security threat is real, and there is strong consensus around the steps that industry must take. Congress needs to do everything it can to drive more effective programs in the private sector. This Subcommittee has extensive experience dealing with complex issues, and we are confident in your abilities to address this one. We are at an inflection point in the effort to strengthen cyber security and need your leadership.

Mr. STEARNS. I thank you, and, Mr. Thompson, thank you for your patience. We welcome your statement .

STATEMENT OF ROGER THOMPSON

Mr. THOMPSON. Good morning. Thank you for allowing me to testify. My name is Roger Thompson.

Mr. STEARNS. Could you pull it a little closer to you, the mike?

Mr. THOMPSON. There we go.

Thank you for allowing me to testify. My name is Roger Thompson. I am the former Director of Malware Research at the TruSecure Corporation, and I am currently Vice President of Product Development at PestPatrol. PestPatrol was founded in May

2000 by a team of software professionals to encounter the growing threat of malicious non-viral software. Currently one of PestPatrol's greatest concerns is the threat of Spyware, so I would like to introduce you to the problem as our customers see it, being consumers, and give you an idea of how the software community's efforts to protect is developing.

Spyware is silent. It is invisible to the consumer. It allows criminals to steal from them. It arrives uninvited and unwanted. It has not received the attention needed to warn the unsuspecting of these dangers to their personal confidential information, and perhaps worst of all spyware and similar malware problems rob consumers of the confidence needed to make commerce over the Internet inviting, safe and successful.

Every day we hear horror stories from our customers that illustrate the very real and personal losses caused by the spyware problem. Wanda Gilman is a church secretary from Saginaw, Michigan. Like most people, she has received warnings from her anti-virus software about virus attacks and she thought she was pretty well protected on that front and unfortunately it became abundantly clear to Wanda that she needed something more after she experienced two instances of identity theft. Neither incident involved more than $1,000, but it was an uncomfortable feeling for her to have her identity hijacked and a long and complicated recovery each time around.

Michelle Scalero from New Jersey has a home computer that her family shares for on-line banking and purchasing, as well as enjoying what the Web has to offer them and their young children. They were extremely alarmed when they found their PC flooded with explicit teen porn pop-ups, caused by a Trojan horse program that had been delivered by a piece of spyware they had unknowingly downloaded onto their computer.

Barbara Wolski bought a brand new computer that was supposed to be very fast, 2.6 gigs, which included a special feature called hyperthread technology to make the processing speed even faster, and then she found that her old computer which was only 1 gig ran faster than the new one. She ran the anti-spyware program and found over 5,000 pieces of spyware factory-installed on the new machine, all busy "phoning home" information about her, causing the massive slowdown.

None of this needs to happen. We hear thousands of similar sad stories all the time. A record number of incidents were reported this year, more than 60,000 at the end of last month and it keeps growing. $24 billion is the estimated identity theft losses in the United States from identity theft last year, $73 billion, estimated identity theft projected domestically by the end of this year, and $9,800 the average take from each identity robbery.

These numbers come from the Aberdeen Group, an industry analyst firm that calls identity theft "the crime that pays." Aberdeen also warns that profits from these crimes are so encouraging that organized crime has become a factor. It has been 20 years since the first virus was created and for much of my career I watched the damage that computers could cause from children at home to senior corporate executives.

My computer career began in Australia in 1979, where I worked as a mainframe systems engineer. I co-founded the first Australian anti-virus software company, Leprechaun Software, and launched the Virus Buster product back in 1987. In 1991, I moved to the United States. I started Thompson Network Software, which produced The Doctor range of systems management and security products.

When I became Director of Malware Research at TruSecure Corporation, I was able to focus more closely on the way that different kinds of malware were developing, and the sheer size of the problem was really brought home to me. Now, at my current company I am working with malware's faster-growing and most insidious incarnation yet, spyware.

Here is the new stuff. The anti-spyware is still in its infancy, but it has proven to me every day from the prevalence data collected by my company that this type of secretive invasive software is a huge problem for computer users. Before we can address possible solutions, we need to define what the spyware problem actually is. For me spyware is any software that is intended to aid an unauthorized person or entity in causing a computer, without the knowledge of the computer's user or owner, to divulge private information.

The industry has begun to make consumers more aware of this threat by banding together. To begin educating the public on spyware and its dangers, we recently co-founded along with several other anti-spyware companies the Consortium of Anti-Spyware Technology, COAST. This nonprofit organization is a forum in which members cooperate to increase awareness of the growing problem. We reached agreement on the definition of spyware, which helps us technology vendors create products that address consumers' concerns. The dangers of spyware are not always known and are almost never obvious. Usually you know when you have a virus or worm. These problems are in your face. Spyware, on the other hand, silently installs itself on the PC, where it might take any number of different and unwanted actions; for example, phone home information about you, your computer and your surfing habits to a third party, to use to spam you or push pop-up ads to your screen, open up your computer to a remote attacker using a RAT, or Remote Access Trojan, to remotely control your computer, capture every key stroke you type, private or confidential e-mails, passwords, bank account information, and report it back to a thief or a blackmailer, allow your computer to be hijacked and attack a third party's computers in a denial of service attack that can cost companies millions and make you liable for damages. They can probe your system for vulnerability to otherwise exploit the system.

If that does not make the computer users on the subcommittee nervous, consider that the on-line holiday season has already arrived. With more and more people shopping on-line, the potential for identity theft is much greater. Shoppers are stressed and distracted and may not take their usual care in protecting themselves from electronic pickpockets.

No one would allow a silent and hidden burglar into his or her home without a fight and, as you saw with the real world experi-

ence I described earlier, spyware has the ability to ruin someone's Christmas. Like having your wallet stolen, life becomes a bureaucratic nightmare of new identity cards and credit cards. And ultimately how do you retrieve your privacy from an unknown or uncaring prowler using the Internet as a hunting ground?

These anti-virus companies were often accused of hyping gloom and doom to help increase their own sales and profits. That was long ago proven to be unfounded. Today, the billions of dollars lost, in identity theft, transaction hijacking, sensitive information, are compounded by the huge losses to credit card companies that must reissue cards whenever an account is compromised or even suspected of being compromised.

The growing threat is no exaggeration. I think everyone on this panel would agree a huge portion of damages and tangential damages caused by spyware and malware goes unreported and is unknown. Something must be done to protect the Wanda Gilmans, the Michelle Scaleros, and the Barbara Wolskis, who only want to conduct their on-line activities and purchases with peace of mind, knowing they can do it safely.

H.R. 2929, the Safeguards against Privacy Invasions Act, is a powerful step in this direction. In person, consumers have the choice not to answer questions when they go shopping. Why shouldn't on-line shoppers have the same choice to say no to spyware. As a representative of my company and as a person who has devoted my working life to malware eradication, I urge you to pass the SPI Act.

[The prepared statement of Roger Thompson follows:]

PREPARED STATEMENT OF ROGER THOMPSON, VICE PRESIDENT, PRODUCT DEVELOPMENT, PESTPATROL, INC. FORMERLY DIRECTOR OF MALWARE RESEARCH, TRUSECURE CORPORATION

Good morning.

Spyware is silent. It's invisible to the consumer. It allows criminals to steal from them. It arrives uninvited and unwanted. It has not received the attention needed to warn the unsuspecting of these dangers to their personal and confidential information. And, perhaps worst of all, spyware and similar malware problems rob consumers of the confidence needed to make commerce over the Internet inviting, safe and successful.

Every day, we hear horror stories from our customers that illustrate the very real and personal losses caused by the spyware problem. Listen for a moment to just three:

- Wanda Gilman is a church secretary from Saginaw, Michigan. Like most people, she has received warnings from her anti-virus software about virus attacks, and she thought she was pretty much protected on that front. Unfortunately, it became abundantly clear to Wanda that she needed something more than her anti-virus after she experienced not one but two incidences of identity theft. While neither incident involved more than $1000, it was an uncomfortable feeling for her to have her identity hijacked, and a long and complicated recovery each time around.
- Michelle Scalero from New Jersey has a home computer that her family shares for online banking and purchasing, as well as enjoying what the web has to offer them and their young children. They were extremely alarmed when they found their PC flooded with explicit teen porn pop-ups caused by a trojan horse program that had been delivered by a piece of spyware they had unknowingly downloaded onto their computer.
- Barbara Wolski bought a brand new computer that was supposed to be very fast (2.6 GHz), which included a special feature called hyperthread technology to make the processing speed even faster. While her old computer was only 1.2 GHz, it ran faster than the new one. Barbara ran our anti-spyware software on the new machine and found over 5000 pieces of spyware factory-installed on

the new machine, all busy "phoning home" information about her—causing the massive slow-down.None of this needed to happen. And we hear thousands of similarly sad stories all the time. Our customers reported a record number of such incidents this year—more than *60,000 as of the end of last month*—and the complaints keep growing.

Here are some numbers to think about as we discuss protecting consumers from spyware:

- 24 billion dollars . . . that's estimated identity theft losses in the US from identity theft last year.
- 73 billion dollars . . . that's estimated losses from identity theft projected domestically by the end of this year.
- 9,800 dollars . . . that's the estimated average "take" from each identity robbery.

These numbers come from the Aberdeen Group, an industry analyst firm that calls identity theft "the crime that pays." Aberdeen also warns that the profits from these crimes are so encouraging that the organized crime is becoming a factor.

You may have heard that last week was a dubious anniversary . . . it's been 20 years since the first virus was created. Through much of my career, I have watched the damage that computer intruders can cause—to every PC user from children at home to senior corporate executives.

My computing career began in Australia (perhaps you recognize the accent) in 1979, where I worked as a mainframe systems engineer. I co-founded the first Australian anti-virus software company, Leprechaun Software, and launched the Virus Buster product back in 1987. After moving to the United States, I started Thompson Network Software, which produced The Doctor range of systems management and security products.

When I became Director of Malware Research at TruSecure Corporation, I was able to focus more closely on the way that different kinds of malware were developing, and the sheer size of the problem was really brought home to me. And now, at my current company, I am working with malware's fastest-growing and most insidious incarnation yet—spyware.

The anti-spyware industry is still in its infancy, but it's proven to me every day from the prevalence data collected by my company that this type of secretive, invasive software is a huge problem for computer users.

Before we can address possible solutions to the problem, however, we need to define what the spyware problem actually is. For me, spyware is any software that is intended to aid an unauthorized person or entity in causing a computer, without the knowledge of the computer's user or owner, to divulge private information.

The industry has begun to make consumers more aware of this threat by banding together. To begin educating the public on spyware and its dangers, we recently co-founded, along with several other anti-spyware software companies, the Consortium Of Anti-Spyware Technology (COAST) group. This non-profit organization is a forum in which members cooperate to increase awareness of the growing spyware problem. We've reached agreement on the definition of spyware, which helps us technology vendors create products that address consumers' concerns.

The dangers of spyware are not always known and are almost never obvious. Usually, you know when you have a virus or worm—these problems are "in your face". Spyware, on the other hand, silently installs itself on a PC, where it might start to take any number of different and unwanted actions. For example:

- "Phone home" information about you, your computer and your surfing habits to a third party to use to spam you or push pop-up ads to your screen
- Open up your computer to a remote attacker using a RAT (Remote Access Trojan) to remotely control your computer
- Capture every keystroke you type—private or confidential emails, passwords, bank account information—and report it back to a thief or blackmailer
- Allow your computer to be hijacked and used to attack a third party's computers in a denial-of-service attack that can cost companies millions and make you liable for damages
- Probe your system for vulnerabilities that can enable a hacker to steal files or otherwise exploit your system.

If that doesn't make the computer users on the subcommittee nervous, consider that the holiday online commerce season has already arrived.

During the holiday shopping season, with more and more people shopping online, the potential for identity theft is much greater—shoppers are stressed and distracted, and may not take their usual care in protecting themselves from electronic pickpockets.

No one would allow a silent and hidden burglar into his or her home without a fight. As you saw with the real-world experiences I described earlier, spyware has

the potential to ruin someone's Christmas. Like having your wallet stolen, life becomes a bureaucratic nightmare of new identity cards and credit cards. And, ultimately, how do you retrieve your privacy from an unknown and uncaring prowler or corporation using the Internet as a hunting ground?

The anti-virus companies were often accused of hyping gloom and doom to help increase their own sales and profits—that was long ago proven to be unfounded. Today, the billions of dollars lost—in identity theft, transaction hijacking, sensitive information—are compounded by the huge losses to credit card companies that must reissue cards whenever any account has been compromised or even suspected of being compromised. The growing threat is no exaggeration. I think everyone on this panel would agree that a huge portion of damages and tangential damages caused by spyware and malware goes unreported and is unknown.

Something must be done to protect the Wanda Gilmans's, Michelle Scaleros's and Barbara Wolskis's, who only want to conduct their online activities and purchases with the peace of mind of knowing they can do so safely. H.R. 2929, the Safeguards Against Privacy Invasions Act, is powerful step in this direction. In person, consumers have the choice not to answer address, phone and email address questions when they go shopping. Why shouldn't on-line shoppers have the same choice to say no to spyware?

As a representative of my company and as a person who has devoted my working life to malware eradication, I urge you to pass the SPI Act.

Thank you.

Mr. STEARNS. I thank the gentleman, and now I will start the questions, and I think I go back to my opening statement.

What are the real risks and costs to consumers for cybersecurity breaches and what poses the most risk to cybersecurity, and then what is the optimum role for the Federal Government to play when it comes to protecting consumers from cybersecurity threats?

I would start out with Commissioner Swindle. You point out in your opening statement that not all security breaches are violations of the Federal Trade Commission. In your opinion, is there a need for legislation in this area, giving the FTC additional authority? What is your feeling here?

Mr. SWINDLE. Mr. Chairman, to the point of not all breaches are security violations or violations of the law, I think if we just think of it in the context of a couple of examples if the breach resulted in my name and address going out to the world——

Mr. STEARNS. That is a breach?

Mr. SWINDLE. [continuing] that is not a problem.

Mr. STEARNS. That is a breach or not?

Mr. SWINDLE. That can be a breach of the system because it is contained in the system, I think, but if along with that my credit card went, that is a serious problem and the consequences could be rather dire if somebody got hold of my financial information, my credit card. Just having my address, which is publicly known personal information, that does not necessarily constitute a violation of law, and I think we could look at it from the context of what harm has been done.

Mr. STEARNS. Do you have a data base in which you have actually collected this information that has internally affected employees or major companies? Do you have a data base at the Federal Trade Commission on this?

Mr. SWINDLE. I am not aware of a data base of that nature.

Mr. STEARNS. Reliable data on harms to data infrastructures caused internally by employees of major data base companies? Do you have a reliable data base?

Mr. SWINDLE. I have never thought of it in that context. I do not think we have a data base specifically designed as such.

Mr. STEARNS. Well, I guess.

Mr. SWINDLE. And assembling that data base might even be setting up a target to be breached and causing a problem.

Mr. STEARNS. What about the Gramm-Leach-Bliley Act? Have you experienced any security problems or policies for financial institutions under the Gramm-Leach-Bliley Act we passed?

Mr. SWINDLE. The problem with that act, the most obvious one, comes from the nature of the requirements for notice, and we have all received the copious quantities of papers that no one could understand. But, I think Gramm-Leach-Bliley has put a focus on institutions' obligation to security and privacy and, in a sense, I think that is good.

Mr. STEARNS. Okay. Mr. Charney, should there be common standards for independent security evaluations and why are such standards important and who should set those standards?

Mr. CHARNEY. For the most part, standards can be important. The risk is that if we set standards that fixate on a particular technology what we will end up doing is stifling innovation. So one of the things that we focus on more is best practices, so that we can develop methodologies in both product development and in management; that is, both at the same time, cutting edge but flexible enough to allow further innovation. So if you are talking about standards for security, for example, there is a risk. For example, the government had a standard for encryption called Data Encryption Standard, and when that standard was no longer viable the entire industry, including the government, moved away from that standard to something more secure, and it was 2 years later that the government finally promulgated a new standard, after everyone had already left the old one. So the challenge is to be able to provide prescriptive guidance to customers and consumers about how to protect themselves without locking in the technology.

Mr. STEARNS. I guess we would say security is a public good. Can markets alone be fully responsive to cybersecurity concerns, just the markets themselves, or——

Mr. CHARNEY. I think the markets have some limitation.

Mr. STEARNS. This best practices you talked about, in your opinion do you think the Federal Government—like Mr. Ansanelli had indicated, there might be a Federal role here?

Mr. CHARNEY. Oh, there is clearly a Federal role and there is a couple of them actually. The government can lead the way in the development of best practices. The General Accounting Office, for example, frequently looks at the security of government systems and issues government report cards which, to be honest, have not been very favorable.

The second thing is there are constraints on the market, and for public safety and for national security purposes governments may need higher levels of security than markets normally provide. In those kinds of cases, the government should take steps, particularly in research and development and other areas, to make sure that the gap between what the governments need and what markets will provide are in fact closed.

Mr. STEARNS. Mr. Ansanelli, you mentioned something about a consumer data security standard that has got our staff's attention,

to ensure that there is a base level of responsibility for consumer protection, consumer data protection.

Do you see the need for this kind of baseline standard and what should the standard be?

Mr. ANSANELLI. The reason why it is helpful to have that standard is when you compare what has happened between Gramm-Leach-Bliley and HIPAA, that those organizations tend to protect data more than other organizations, so you have seen improvements as a result of the security requirements and Grammm-Leach-Bliley, I think it is section 501(b), with respect to protecting consumer data. So there have been improvements in the protection of that data as a result, and I think that evidence indicates that it would be better to also then have other organizations that actually keep that same data, if a financial institution has my Social Security number, when I buy a phone if I have to give them my Social Security number because they do a credit check on me. So why is it that one industry might have to have a standard where another might not, and I think very importantly the risk that I think might happen is that the States will end up driving the requirements and the regulations, so that either companies will have to wind up dealing with a patchwork of lots of different regulations. There are about 200 different identity theft bills at the State level currently being discussed right now. I think it is important there is a uniform standard as opposed to 50 different standards that has to emerge.

Mr. STEARNS. So what you are saying is you would like the Federal Government to come up with the consumer data security standard?

Mr. ANSANELLI. Yes, and it should be about what are the best practices and what are the requirements that every company who stores non-public personal information should have to live by and it should be something that——

Mr. STEARNS. Mr. Burton, would you like to comment and then I will close?

Mr. BURTON. Yes.

Any of that is working on standards. I guess it is my concern that by treating it as a technical issue, which standards again puts you squarely back into a technical discussion, you are missing a huge motivator here, and that is that senior management is not making the decisions to invest, to train, to hold people accountable, because it is extremely complex and it is too often seen as a defensive technical issue.

A porcupine if it rolls itself into a ball is perfectly protected. Its quills are everywhere, but they cannot move, they cannot eat, they cannot do anything productive, and I think so much of this discussion is on definitive technology issues that fail to address the management question and the issue that ultimately a lot of cybersecurity is enabling, just as quality is enabling, and I think you can make a huge contribution.

Mr. STEARNS. Thank you.

Ms. Schakowsky.

Ms. SCHAKOWSKY. Mr. Swindle, I wanted to get back to your comment that you made, regarding the fact that if my name and address went out that that is not a very serious breach of security,

and so some things are serious and some things are not, and yet when you look at your testimony and you talk about the Commission's first information security case, the Eli Lilly case, which essentially was the name and address, in this case an e-mail address, but in any case it was consumers of Prozac—was it? Yeah, Prozac, very sensitive information, and all that went out was a name and address. So I am disagreeing with you that name and address going out is not necessarily, or certainly can be an important breach of violation, I would think, since you treated it that way. But I also was concerned about the sanctions, which seem to me a very minor slap on the wrist, whereas the implications for consumers of that information, that very sensitive information going out, could be very serious. So I wanted you to just comment on this.

Mr. SWINDLE. I would be happy to, Congresswoman.

First off, I believe the question related to there could be a breach without a violation of the law. I believe that is the way I understood the question.

The release of nothing more than my name and address, which is in the phone book, could hardly be construed as a violation of law.

Now, in the case of Eli Lilly, it was a name and the address and the identification of a person who was using a medication. The use of that medication carries a connotation of health problems and all sorts of emotional problems perhaps and things of this nature, which could indeed be certainly a gross violation of personal information and privacy. So that can be construed, I think. They are entirely two different things if we take them in the context I gave them to you. But perhaps another way of looking at this: How can there can be a breach without a violation of the law?

We are dealing, if I may describe this as an example, we are dealing with a machine with a million moving parts in it and to my mind nobody's perfected all one million parts, and companies can take every reasonable effort they know how to take, given the circumstances of the nature of the information and how it is stored and how it is used, and there might still be a breach in the security.

Having taken every reasonable step they can take, then I think we would probably find it hard to say that is a violation of the law, when they did everything they possibly could. As technology evolves we will constantly be confronted with that problem. You know, the Defense Department has this problem, Congress has this problem, Microsoft has this problem, all companies have this problem because it is just a massive complex problem with which to deal. I do think there is a distinction there.

Ms. SCHAKOWSKY. Are you talking about, what did you say, user error? Are you talking about perhaps issues of management, individual errors that are made? I mean, it would seem to me that a company would still or anybody would still have to take responsibility for that. I am trying to understand where you draw the line.

Yes, we certainly expect that all possible measures are taken, and you are saying but if there is still a breach after that, then nobody is responsible for that?

Mr. SWINDLE. No, I do not think I said that, Congresswoman.

Ms. SCHAKOWSKY. Okay.

Mr. SWINDLE. I did not address the accountability. We all have to be accountable. We are responsible for running the train, and I think industry does take that responsibility very seriously.

In the case of Eli Lilly, we thought that the best possible solution. This is an incredibly fine company, as is Microsoft, as are the companies represented here on this panel. They are doing their utmost.

In the case of Eli Lilly, there was negligence, not sufficient training, there were not sufficient technical safeguards put in. They are under scrutiny and have corrected those requirements, the deficiencies, and we are going to be monitoring them. As I think I indicated, they report to us with an audit system every 2 years.

Ms. SCHAKOWSKY. Yeah, I would still think that it is more than a slight slap on the wrist.

Mr. SWINDLE. And we were concerned with this, but what do we—what else perhaps—questionably, what else could we have done?

Ms. SCHAKOWSKY. That is the question for us; is not it?

Mr. SWINDLE. A huge penalty, would it accomplish that and correct the problem?

The problem was mostly technical and training, I think. If they corrected the problem, we go on. They certainly can be subject to several penalty pursued by the people they harmed. That is always open to victims.

Ms. SCHAKOWSKY. Well, I think much of the testimony here does say that there need to be appropriate sanctions, and that is certainly what we need to consider.

I want, Mr. Chairman, to have your permission to leave the record open for further questions. I have a number of questions.

Mr. STEARNS. I think that is in order.

Ms. SCHAKOWSKY. If I could put in?

Mr. STEARNS. Sure.

Go ahead.

Ms. SCHAKOWSKY. I wanted to ask—I wanted to submit this document, which is an e-mail from Bill Gates and addressed to Microsoft and subsidiaries. They are all FTE dated January 15, 2002, for the record, and I have a number of questions around that that I hope that Mr. Swindle will answer, and also actually Mr. Charney, about that.

Mr. STEARNS. Would you like to submit that?

Ms. SCHAKOWSKY. If I could.

Mr. STEARNS. By unanimous consent, so ordered.

[The information referred to follows:]

From: Bill Gates
Sent: Tuesday, January 15, 2002 5:22 PM
To: Microsoft and Subsidiaries: All FTE
Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing—or able—to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft .NET more than two years ago, we set a new direction for the company—and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy Computing. What I mean by this is that customers will always be able to rely on these systems to be available and to secure their information. Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.

Today, in the developed world, we do not worry about electricity and water services being available. With telephony, we rely both on its availability and its security for conducting highly confidential business transactions without worrying that information about who we call or what we say will be compromised.—Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

The events of last year—from September's terrorist attacks to a number of malicious and highly publicized computer viruses—reminded every one of us how important it is to ensure the integrity and security of our critical infrastructure, whether it's the airlines or computer systems.

Computing is already an important part of many people's lives. Within ten years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.

Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched—but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.

No Trustworthy Computing platform exists today. It is only in the context of the basic redesign we have done around .NET that we can achieve this. The key design decisions we made around .NET include the advances we need to deliver on this vision. Visual Studio .NET is the first multi-language tool that is optimized for the creation of secure code, so it is a key foundation element.

I've spent the past few months working with Craig Mundie's group and others across the company to define what achieving Trustworthy Computing will entail, and to focus our efforts on building trust into every one of our products and services. Key aspects include:

Availability: Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level—from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

In recent months, we've stepped up programs and services that help us create better software and increase security for our customers. Last fall, we launched the Strategic Technology Protection Program, making software like IIS and Windows .NET Server secure by default, and educating our customers on how to get—and stay—secure. The error-reporting features built into Office XP and Windows XP are giving us a clear view of how to raise the level of reliability. The Office team is focused on training and processes that will anticipate and prevent security problems. In December, the Visual Studio .NET team conducted a comprehensive review of every aspect of their product for potential security issues. We will be conducting similarly intensive reviews in the Windows division and throughout the company in the coming months.

At the same time, we're in the process of training all our developers in the latest secure coding techniques. We've also published books like "Writing Secure Code," by Michael Howard and David LeBlanc, which gives all developers the tools they need to build secure software from the ground up. In addition, we must have even more highly trained sales, service and support people, along with offerings such as security assessments and broad security solutions. I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute.

But we need to go much further.

In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve.— A good example of this is the changes we made in Outlook to avoid email borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen, and we must be the kind of company that people can rely on to deliver it.

This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

BILL

Mr. STEARNS. Let's see, the gentlelady from California is recognized.

Ms. BONO. Thank you, Mr. Chairman, and I thank the panelists for sticking with us through all of this.

I think the one theme that generally has come up for me in this testimony so far is that Ms. Davidson alluded to the fact that California did some knee-jerk reacting to the situation and came up with legislation that was not very good, and whether or not you know this, Congress is probably—in all of the issues we deal with we are technologically challenged, and we were all thrilled the day we got Blackberrys, but there is a funny story I remember of a Member of Congress who held up his Blackberry and said this is great, I do not know how to work it, and I said why don't you try turning it on first, and that is a true story.

Now, these people might be experts in whatever field they are in, we have the CDC and the NIH, who do a lot of our great work in medicine, but in Congress do we have the governmental entity in place?

I think, Mr. Swindle, I would ask you the question. We have got the FTC, the FBI, but do we have an entity that works specifically with Congress to move more swiftly in the case of these issues or is it sort of—are we a little bit lacking in that area?

Mr. SWINDLE. I do not think we have a central agency that would combine the resources of all of us to work with Congress, but I think each of these agencies, in their own realm, work with Congress very closely. I know we try to work with Congress as closely as we can when Congress is considering drafting legislation to solve a problem. Often we propose suggestions as to how current laws might be modified, and I think we are often on the side of urging caution before we legislate to solve a problem where very likely the proposed solution will perhaps cause more harm than good. As one of the panelists said earlier, sometimes the process is so slow that we have gone well beyond that problem and already found a solution to it.

In all honesty, I think it takes each one of these agencies. They have some responsibility and oversight of these issues, dealing with their expertise, working with Congress, and realizing that there is no simple solution to any of these problems.

Legislation alone will not solve it, technology alone will not solve it, and in my mind the most important single factor when you think of the base of the triangle of people who are involved, the consumers across the bottom, 270 million. As we work on up to the triangle top we are worrying about nuclear attack, but that is only a handful. But down at the bottom of this triangle, every one of the people in the base, consumers, students, business people, small business people who are using computers and are connected on the Internet, they are all part of the problem and part of the solution.

Ms. BONO. Right. I am sorry for cutting you off, but my spyware legislation, I think you have seen it or your staff has seen it, and I was wondering if you could comment because to me this seems to be a good solution. It seems to address the situation.

There have been some, you know, tremendous media reports, and I thank the media actually. Even The Washington Post today has a great article and in it he quotes something that shocked me. I do not believe anybody brought this point up. I have it here, I promise you.

Anyway, he talks about—here it is, Sharman Networks, that when you download KaZaA, that they install something called ALLNET and that this ALLNET actually harnesses unused processing power on your CPU and then sells that processing power. I have never heard of sharing hardware over this and I am wondering if perhaps, Mr. Charney, you could comment on the fact that they are not only using data but they are basically stealing a little bit of your processing capability.

Mr. CHARNEY. The key word there is stealing, so one of the things we need to be clear about is that peer-to-peer networks have some important societal advantages. You look at something like SETI, the Search for Extraterrestrial Intelligence, where a lot of

independent researchers and individuals agree to share processing time because what happens is that computers have become far more powerful. Home users have a lot more power on the desktop than they actually use or need, and one of the issues is can we harness that process in some way and share that power.

The key is that those things have to be done with full notice and consent and not done to someone without their knowledge, where someone else is either taking their information or processing power without telling them, without getting their consent. But it would be a mistake to think that peer-to-peer in and of itself is a bad thing.

Ms. BONO. Right.

Mr. CHARNEY. Merely the technology that permits the use of distributed processing.

Ms. BONO. Well, is Microsoft concerned about spyware? Other than pretty much endorsing my bill, thank you for that, if that is what he was doing, Mr. Chairman.

Mr. CHARNEY. We absolutely care about spyware, so one of our pillars of trustworthy computing is privacy, and our philosophy is that consumers have to make informed choices of how data is used and to be able to control the data about them, and to the extent people are taking their data without their notice and consent, that is a problem, and the solution, like most IT solutions, will be a combination of best practices, technology, and in some cases regulations.

Ms. BONO. Could the ISPs do a better job? I know you all have MSN, but obviously they are not going to, but could not, for example, your competitor, AOL, who promotes McAfee daily, every time you log on you get this sales pitch from McAfee, could not they install that along with their software, AOL, and have it built into the firewall and the automatic patches that you say consumers do not do often enough?

Mr. CHARNEY. We have tried to make this easier for consumers. We have built the ICF firewall into Windows, and if you go to the Microsoft.com/protect, we have links to anti-virus vendors, where people can easily get virus software. We have to make it much easier to manage.

I would point out that you have to remember this technology was built by geeks for geeks. If you think about the telephone as phones ended up in every home in America, the phone company said if we are going to sell more services, we have to devise more complex software, call forwarding, caller ID, all those features. As they add all this complexity, the user interface remained the same, 12 buttons.

My mother has a PC. She is 74 years old. She can go to a run command, write her own code and run it. She cannot, she is not technically capable of doing it, but we have given her the technology to do it. It is a completely different paradigm.

Ms. BONO. Thank you. Mr. Chairman, I will yield back.

Mr. STEARNS. We are going to have a second round if you want to.

Ms. BONO. Thank you.

Mr. STEARNS. I recognize the gentleman from Arizona.

Mr. SHADEGG. Mr. Ansanelli, you mentioned in your written testimony an unaddressed issue regarding identity theft in the Fair Credit Reporting Act, the legislation that is in conference that I referred to in my opening statement.

Can you go into greater detail about that?

Mr. ANSANELLI. Sure. It has not been passed yet by the whole House and the Senate, but I think if you look at what the Fair Credit Reporting Act has in it, I think about the issue of identity theft as sort of three pillars.

The first is protecting the data that is the consumer's identity to begin with. Second is detecting any problems that are occurring, either someone is trying to do fraud or, you know, trying to get a credit card as a result of fraud. And then the third thing is correcting the problem, primarily for consumers. How do consumers fix their credit? They have been a victim. How do they correct it?

And as I look at the act there is quite a bit in correcting the problem for consumers, and that is good. There is a fair amount of detecting the problem with respect to address notifications and what not, but there is very little with regard to prescriptions for protecting information to begin with, and that goes again to the issue around consumer data standard, and if you do not protect the data you are only going to have to apply larger and larger BandAids in the future.

Mr. SHADEGG. I tried to amend that legislation to add further restrictions on the use of Social Security numbers. However, had we done that, it would have taken it out of the jurisdiction of the Financial Services Committee and put it in the jurisdiction of the Judiciary Committee and it would have caused the bill to require a second referral and we weren't able to do it, but would you agree that that is one of the most important things that needs to be done?

Mr. ANSANELLI. I agree that that is a glaring omission.

Mr. SHADEGG. The gentlelady sitting next to you, it seems you would like to make a comment on that point?

Ms. DAVIDSON. Hosanna. I was making a note to myself that no one—although you did ask the obvious question why is the Social Security number collected in so many nontaxable transactions. Having recently purchased a house in the great State of Idaho, I was astonished to find that every single entity in the city, whether it was sewage, power, trash pickup, required my Social Security number and I had to ask the question: Is sewage taxable, because it was a complete mystery to me why it was collected in the first place.

The Social Security number, had it not become ubiquitous as a means to identify consumers, quite honestly, a lot of the identity theft problem would probably go away.

Mr. SHADEGG. My colleague, Clay Shaw, has a comprehensive bill addressing this issue, going right to the issue of Social Security numbers. That was the issue we would have tread on if we had been able to put further restrictions on Social Security numbers into the Fair Credit Reporting Act, and that is the reason we did not do it. You might want to contact his office and interject yourself into the debate on that bill because I think that is an important part of this discussion.

We were able to require the truncation of Social Security numbers in the draft of the fair credit reporting bill that passed the House. We did that, so we have taken a minor step, but I think it is a serious problem.

Mr. Ansanelli, Mr. Burton next to you says we shouldn't be looking at these technical issues and creating a standard. We ought to be instead creating incentives to do that.

I am going to give him a chance to explain that, but how do you respond?

Mr. ANSANELLI. I agree. I am not proposing we have technical requirements or standards. I think the standards need to be around principles, and as I testified today, and I did testify in the House Financial Services Committee on FCRA, that it involves responsibility from everyone at the board level down to protect the data and you have to have those principles to make sure that everyone knows they are responsible for protecting the data, that they have an obligation to detect and enforce compliance by the people that have access to the data and you need to correct problems, and the correction of those problems includes things like training and education. It is definitely not proposing technical standards. It is having a clear understanding of the responsibility associated with the fact that you store and manage that consumer non-public, private information.

Mr. SHADEGG. With regard to the protection of information where you think we could have gone further in the Fair Credit Reporting Act, would you be willing to submit to my office your suggestions as to what we need to be doing to go beyond that?

Mr. ANSANELLI. More than willing.

Mr. SHADEGG. I have some doubts about the ability of Congress to micromanage this problem, legislative piece by legislative piece.

We passed the Identity Theft Act a number of years ago, and it took a step in the right direction, but we are not there. It seems to me that crooks are always going to move faster than we are and we are not going to be able to achieve the kind of reform or the kind of protection we would like to just by legislating one bill at a time in this area. So your notion that business needs to take a completely different mindset seems to me a better solution.

How do we go about creating the incentives or creating a dynamic in which business leaders will see it as in their interest to not act like the porcupine and roll up in a ball and defend itself, but rather aggressively go after this problem?

Mr. BURTON. That is a seminal question, I think, and I think that is a question that industry needs to ask itself, as well as this committee needs to reflect on, because to go back to Scott Charney, if the PC is something built by geeks for geeks, well, then cybersecurity is the pinnacle of the geekiness in the PC, and I think when this issue comes up, too often the reaction is oh, mine eyes glaze over. I will talk about privacy, that is a personal issue, that is a consumer issue, and I can understand it. Cybersecurity is a geek technical issue that I do not want to even open that book, and I think that if we somehow make the translation from a technical issue, and it is technical, I am not saying we should dismiss that, but it is often treated solely in those terms, and again the best paradigms that I have is quality, and quality awareness comes

first, I think we have awareness with cybersecurity. Now we need to start building it systematically and to functions of our system, and I think anything this committee can do to clarify cost-benefits and perhaps penalties would be a big contribution, and again I think the levers are not that complex. I think it is risk assessment, it is reporting, it is accountability, and I think those three opinions can really drive huge, huge change in this field.

So I do not have a specific answer for your question, but I do think that is the key question for this whole debate.

Mr. SHADEGG. Mr. Chairman, my time has expired. Thank you.

Mr. STEARNS. Thank you.

Members, if you want to stay, we will have a second round.

The gentlelady from Missouri.

Mr. MCCARTHY. Mr. Chairman, let me apologize for having to leave. I had another hearing and of course when you do that, the question that you are going to ask might have been asked already. So, Mr. Chairman, please feel free to say read the record.

Microsoft, let me just see. I think I want to give this to Ms. Davidson, I think might be in the best position to answer it.

Microsoft Corporation made news when they announced a bounty program for information leading to the arrest and prosecution of hackers. Do you intend to launch a similar program for those hackers who attack your software?

Ms. DAVIDSON. That is a very interesting question. We have no immediate plans to do this, and I preface this statement by saying I have no wish to exceed Microsoft in this particular realm. Microsoft tends to be a very visible target for hackers, to be fair to them, because they are large, they have been very successful, and, quite honestly, there are more hackers gunning for them at this point than are gunning for Oracle, for which I am exceedingly grateful. I am happy to accede market leadership to you in that realm.

At this point, I do agree with certainly Microsoft and others in the industry on one key point. We certainly welcome people who find faults in our software and bring it to our attention. We certainly do everything possible to avoid them the way that we build our product, and we are always happy to give recognition to those researchers who find fault and say thank you, we have fixed it, and we tell our customers.

There are a group of researchers for whom thank you and potentially hiring them for bettering your software is not enough. They want your scalp, and one of the ways they get that is by releasing exploit code at forums such as Black Hat and other hacker conventions.

No vendor will say that it is not their responsibility to build secure software. The buck definitely stops here, but those who trade in information about how to exploit vulnerabilities and give it to others are effectively arsonists swapping fire starting techniques, and they claim they want better building codes but try telling that to someone whose house has burned down.

So at this point we have no plans to offer a bounty, but I do agree that the problem of irresponsible disclosure of detailed information about security faults, specifically creation of exploit code and releasing it into the wild, is in part responsible for a lot of the malicious and damaging behavior to our infrastructure.

Mr. MCCARTHY. All right. Does open source software like Linux have vulnerabilities to worms and viruses?

I have seen a recent report that an open source developer tried to insert a Trojan horse into Linux.

First of all, could you explain what is a Trojan horse, and how do you ensure that your developers do not insert malicious codes like that into your data base?

Ms. DAVIDSON. A Trojan horse is—of course, goes all the way back to Greek literature in the Iliad, actually the Odyssey. The idea is to get something into your code base that does something malicious. For example, one could insert code that would capture a user's password and potentially mail it to a bad guy or capture a Social Security number or other sensitive piece of information. The premise is that someone has deliberately and willfully put code in that does something bad, unbeknownst to anyone else.

This is something people spend a lot of time talking about and it is certainly not—it is a risk but, quite honestly, most of the problem in software that creates these viruses and worms is preventable, avoidable security faults.

I mentioned, and I will not get all nerdy on you, but buffer overflows. That is about 70 percent of security faults, and it basically means that instead of—if a program is expecting 10 numbers and it does not handle gracefully if it receives 11 numbers, or letters or something else, it could create a buffer overflow and that is 70 percent approximately of security faults. It is just bad programming.

So getting back to your question how do you prevent this——

Mr. MCCARTHY. Yes.

Ms. DAVIDSON. [continuing] I believe you cannot absolutely prevent someone from willfully putting malicious code in your software because you cannot prevent them from making careless errors. Now what you can do is to have very good development processes, you can have code reviews, you separate your code so that not everyone gets access to everything to make changes, and the one piece that truly is missing right now is we do not have automated tools that can scan code and find, first of all, avoidable, preventable security faults, which is really most of the problem in that, much less look for things like malicious code or malware. The tools just do not exist in the market now.

Mr. MCCARTHY. Thank you very much, Mr. Chairman. I see my time has expired.

Mr. STEARNS. I thank the gentleman.

Mr. Morrow, you summed up your testimony by characterizing, "our state of information security readiness is marginally better than it was 2 years ago."

What can we as the U.S. Government do so that 2 years from now the improvement in our information security readiness would be more than marginal?

Mr. MORROW. Well, sir, I believe I outlined a few things in my testimony. One of the things that we see a lot of is that a lot of effort has been spent by very large organizations, the financial industry, you know Fortune 500 companies, but a lot of the issues have trickled down and a lot of the vulnerabilities are still being addressed at the levels of the mid-range business and the small-

range business, and that is for several reasons. One, these things cost money to fix. A lot of companies in the last few years due to the economic downturn haven't had the money to invest in these type things, and you have to understand and always keep aware of the interconnected nature of all these things, and just because the Fortune 500 companies and the government may make great strides, if the smaller companies and smaller institutions, private organizations, et cetera, do not make similar strides, cannot make similar strides for economic reasons, then there is a problem because that opens up vulnerabilities to everyone.

So I think one of the things personally that we can have a lot of bang for the buck, if you will, is to help figure out incentives for small and mid-size and smaller companies to—and organizations to address these problems.

Mr. STEARNS. Who would provide these incentives?

Mr. MORROW. Well, I think it could be a couple of different ways. One could be financial incentives of some manner. That obviously is something in the purview of the Federal Government. Others might be the research and development, tax credits, things like that, and there may be an education or some sort of public service type of incentive where very small companies who offer—small tier companies and small businesses, privately owned businesses, who have one or two systems and have problems, they may require incentive from the government to provide them with basic tools, much like what Microsoft does in some of their software, for a very much reduced cost. I think that would go a long way.

Mr. STEARNS. Okay. Mr. Schmidt, to date how effective have cyberattacks been, and have you seen an increase in their effectiveness, and, if so, why do you think so?

Mr. SCHMIDT. I think first and foremost we have to define what we mean by how effective they have been. For example, if the intent of some of these were to shut down major financial systems, shut down electrical power grids, no, they have not been successful on a universal basis. We have seen some spot outages. But, as we move forward, I think what we will see is the—as we referred to as the zero-day vulnerabilities and exploits. As both Ms. Davidson and Mr. Charney mentioned, the time between the identification of vulnerability and the time that it is exploited has been increasingly shorter.

Now, you mentioned in your opening comments, Mr. Chairman, the SQL Slammer event back in January. That widespread event took place in less than 10 minutes, whereas some of the ones you mentioned earlier, the Code Red and Nimda, occurred over a matter of days to see maximum infection.

The interesting piece of this is if you look at the ratio of computers affected versus the ratio of computers that are now currently employed, it was actually a smaller percentage of computers that were infected in a shorter period of time, but we have got a lot more computers out there. So we are doing a better job at it. So overall, the impact was probably less than it could have been had it been 2 years ago with that same number of computers.

I think the fundamental issue is if we don't continue to improve these processes, reduce the vulnerabilities, make better tools available to prevent these things from even taking place, which, as the

Department of Defense has shown, 98 percent of the successful intrusions into those systems were the result of someone not installing a patch, so if we install the patches, their effectiveness would be much less than they are today.

Mr. STEARNS. Ms. Davidson, I think you recommended a government software underwriters lab. I think that intrigued all of us here and the staff, sort of the consumer equivalent of—software equivalent of the UL. I would like you maybe to elaborate and then have the Commissioner maybe just give his comments on it.

Ms. DAVIDSON. Thank you. I would be happy to do that.

We do have mechanisms for large pieces of commercial software to go through an independent security evaluation. There is an ISO standard for that, 15408, which is a common criteria.

As I mentioned earlier, the Defense Department requires products used in national security systems to go through common criteria evaluations. They are really good, and they help improve the security of software, because it forces developers to a secure software development process. That is a great thing, and we are a great proponent of that. But they are best suited—it is certainly not a cure-all for all cybersecurity ills, and they really are best suited to more mature products with a longer life cycle that are really sort of large pieces of software, like operating systems or data bases, firewalls. That is not—and they are quite expensive. They can cost between $500,000 and $1 million.

That is obviously not well-suited for a small consumer products device, where the cost of the evaluation might actually dwarf your product sales. Usually something is better than nothing when you are talking about improvements. If you can have something that is a lighter weight form of that for commercial products, like a PDA or other types of small devices, that would be——

Mr. STEARNS. I talked to a president of a university, and he said he is going to have to spend $100,000 for software to protect his university from cyberattacks. So maybe that piece of software should go to a software underwriters lab. Is that what you are saying?

Ms. DAVIDSON. Well, I think you have to look at probably the complexity of the software, the target market, and what it is being used for.

Mr. STEARNS. So cost alone would not determine?

Ms. DAVIDSON. Cost alone doesn't. And as much as people complain about how expensive these are, I can tell you that it costs Oracle—if we have a security fault in our software that has been out there a few years, and we have to fix it on 20 operating systems and four product versions, which we have done to protect all our customers, happily to do that, it costs us $1 million to fix that type of avoidable, preventable security fault.

If you prevent one of those or find it before you ship the product, you pay for the cost of the evaluation.

Mr. STEARNS. Uh-huh.

Ms. DAVIDSON. So it is cost-effective. And risk management doesn't really work when you are talking about, well, I am going to let my customers hang in the wind because I didn't feel like doing a better quality job with my product. That is not acceptable.

Mr. STEARNS. Commissioner, what do you think of the idea of a software underwriters lab? I mean, it wouldn't necessarily be under the Federal Trade Commission, but you are the only person here from the government, so we will ask you.

Mr. SWINDLE. In this entire world of information technology we live in, I think creative ideas are going to be the currency of making progress. And I think any idea of this nature deserves attention, as Ms. Davidson said.

These remedies that we often aspire to are very expensive, not to mention the fact that they are very complex. I think we are always interested, the FTC, in exploring new ideas.

Something that I would suggest that deals with most of the questions that have been asked, that is security, sort of mirrors the privacy debate that we have had over the last 5 or 6 years that I have been at the Commission. If you go back 6 years ago, very few companies had privacy policies. They didn't post them. They were not very effective or were too difficult to understand. Today that has changed appreciably. And I used to say that privacy had better become a part of the corporate culture of businesses or there would be an FTC in their future, probably.

I think security is along the same track, just running a few years behind. Security has got to become an essential part of the management scheme of all companies, because we are becoming more and more reliant upon handling of data and information and the transmission of that data and information. Without security, we jeopardize the whole system. It becomes a matter of critical importance to one's own self-interest that we do this right. So I think security is going to have to become a part of the corporate culture as well as privacy.

Mr. STEARNS. Okay. Let me just conclude, Mr. Thompson. We want to make sure you are involved here. Maybe just you can give a general evaluation on cybersecurity relative to this spyware that Ms. Bono has mentioned, maybe just some general comments.

Mr. THOMPSON. Sure. I think I have heard some great ideas and some great suggestions. The only thing is that it has really all been aimed at protecting the corporate end of things, and protecting the consumer from the corporate end of things.

But there is more to it than that. There is a whole world of consumers out there, and there is no one standing up for them. That is really the intent of Ms. Bono's bill. Every month I see thousands of Remote Access Trojans posted to the Usenet in an attempt to catch some of these consumers, and there is no—they are catching people, and there is no one sticking up for them.

Mr. STEARNS. Every month you see thousands?

Mr. THOMPSON. Thousands of Trojan horses are disguised as adult movies or——

Mr. STEARNS. Help aids?

Mr. THOMPSON. Something. And they are posted to the Usenet. They are posted to the peer-to-peer networks.

Mr. STEARNS. So you download that, thinking this software is going to help you. Bingo, you are caught.

Mr. THOMPSON. And are you caught. And these are the worst kind of spyware. These are the ones that do steal the keystrokes, these are the ones that do steal your credit cards, they do steal

your identity. And no one is looking out for these people. Someone has to look out for them.

Mr. STEARNS. My time has expired.

The gentlelady from California.

Mrs. BONO. Thank you, Mr. Chairman. I want to piggyback on that for Mr. Thompson as well. If you installed something like Norton Utilities or an antivirus firewall, every time your computer transmits to the Internet, you can have a notification that tells you your computer is speaking to the Internet.

Mr. THOMPSON. Sure.

Mrs. BONO. Does that, in fact, notify you that spyware is transmitting data?

Mr. THOMPSON. If everyone is playing by the rules. But sometimes they are subtle and they simply don't play by the rules, and they piggyback on something that has already been authorized. These things are tricky.

Mrs. BONO. Some people have said that the problem with this legislation is companies would move offshore, similar to the antispam legislation. But, to me, this doesn't seem like a valid argument. Would you——

Mr. THOMPSON. I think some of them are offshore already, and probably some more would move offshore. But it would be nice to cut down on the people that were actually doing it openly.

Mrs. BONO. I agree. Thank you.

Ms. Davidson, you briefly mentioned hacker conventions or conferences. Is there a room filled with people at a Hyatt doing this, or is this something that is all taking place online?

Ms. DAVIDSON. I think they are a little more upscale than the Hyatt, no disrespect to Hyatt.

Yes, there are such things. I am sure that Mr. Charney has been to one as well to see the amount of collusion going on in the halls to try to exploit the latest vulnerability in vendor software.

Quite honestly, some of the hackers spend more time in the hall devising viruses than I think they do at the actual sessions. There are such things. One of the problems in the industry really is that the hackers are very good at playing nicely with one another. They share information. They share exploit code.

One of the reasons there is such a shortening of this window is in the past you could assume if there was a vulnerability in your software, and it was difficult to find or exploit, someone would have to spend a lot of time doing that. Then you only had to worry about the one bad guy or bad gal as the case may be. Now those people create automated ways of doing bad things, and they share it with other people, who may then improve upon it and find more destructive or virulent forms of viruses or worms. And they actually have conventions. That is a real problem.

Mrs. BONO. That is amazing to me that we can have physical get-togethers of bad guys, and they are infiltrated by the FBI or whoever ought to be there. How do we not know about this but you guys do?

Ms. DAVIDSON. Well, I think—Scott, I am sure, will have some comments on this. Actually there are a number of people who go to these from industry, partly because that is where they learn about the latest techniques for breaking into things.

I am not against general discussions of how to—how things are broken so that you can understand how to better defend against those attacks. I think we would be sticking our heads in the sand if we didn't participate in that. But when someone creates the exact—effectively leaves a Molotov cocktail on the front lawn of a building with a box of matches next to it, with a sign that says, have fun throwing this, they have some accountability. And many of them feel that they have no accountability; it is intellectual showing off.

Mr. CHARNEY. I want to add a couple of comments, because I think they are important. I spent 9 years as Chief of the Computer Crime and Intellectual Property Section at the Justice Department. Law enforcement agents do go to these conferences. They actually have a Spot-the-Fed event, which is quite common.

But there is something else that is also important to note. I mean, I agree with all Mary Ann's comments, but after the Oklahoma City bombing, the Office of Legal Council gave a constitutional opinion, at Congress's request, that bomb-making information on the Internet was first-amendment-protected.

Similarly, information about code vulnerabilities, exploit code, other kinds of information like that is constitutionally protected most likely. It is one thing to deploy the code and take action, but to go to a conference and talk about how you might exploit a system is probably a constitutionally protected activity.

And so we always have to keep this in some context.

Ms. BONO. Thank you.

Is there any—changing the subject a little bit, recognizing that the minute that something is digitized, it is a 1 and a zero, but are there hardware answers here like biometric identifiers or credit card terminals that hardware manufacturers are looking at? And I am basically back to consumer protection solely, but is there a hardware answer on the horizon?

Mr. CHARNEY. Microsoft is investing about $6.9 million this year on research and development, and one of the more important projects we are working on is something called the next generation security computing base. It is moving security into the hardware, working with the major chip manufacturers to create a secure chip set on your computer. You will still have the general purpose computer that you have today, but you will have a second chip set that will control what runs on your machine with strong memory and process isolation.

And the goal of this, if this works, is that when code tries to execute on your machine without your permission, if it is on that protected side of the machine, you will be notified that code is trying to run. You will be able to block it.

But, this is, you know, very difficult research and development. And, I mean, we are shooting for, in the long-term timeframe, the next version of the operating system, which means roughly 2006, give or take.

Mrs. BONO. Well, thank you.

Mr. Chairman, I can go on and on, but I will stop. I just thank you all so much for your time today. It has been very informative.

Mr. STEARNS. And I thank the gentlelady for staying for the second round.

We have concluded our subcommittee hearing.

I would point out that the Federal Trade Commission has a complete set of documents talking about how to stay safe online. They have a little mascot who is promoting it. And so I call attention to Members, too, that part of these programs probably should be on their congressional Websites so people can go to use, whether you are sight-seeing on the Internet or whether you are talking about electronic theft, or how to stay safe. The Federal Trade Commission has done a great deal of work on this and are to be commended for all that they are doing.

With that I want to thank the witnesses, and we will probably have some follow-up questions for you. And I will allow the members to offer that to you, give you 5 working days to answer them if you could.

With that, the subcommittee is adjourned.

[Whereupon, at 12:20 p.m., the subcommittee was adjourned.]