

COMPUTER VIRUSES: THE DISEASE, THE DETECTION, AND THE PRE- SCRIPTION FOR PROTECTION

HEARING

BEFORE THE

SUBCOMMITTEE ON TELECOMMUNICATIONS AND
THE INTERNET

OF THE

COMMITTEE ON ENERGY AND
COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

NOVEMBER 6, 2003

Serial No. 108-66

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

90-727PDF

WASHINGTON : 2003

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	JOHN D. DINGELL, Michigan
JOE BARTON, Texas	<i>Ranking Member</i>
FRED UPTON, Michigan	HENRY A. WAXMAN, California
CLIFF STEARNS, Florida	EDWARD J. MARKEY, Massachusetts
PAUL E. GILLMOR, Ohio	RALPH M. HALL, Texas
JAMES C. GREENWOOD, Pennsylvania	RICK BOUCHER, Virginia
CHRISTOPHER COX, California	EDOLPHUS TOWNS, New York
NATHAN DEAL, Georgia	FRANK PALLONE, Jr., New Jersey
RICHARD BURR, North Carolina	SHERROD BROWN, Ohio
<i>Vice Chairman</i>	BART GORDON, Tennessee
ED WHITFIELD, Kentucky	PETER DEUTSCH, Florida
CHARLIE NORWOOD, Georgia	BOBBY L. RUSH, Illinois
BARBARA CUBIN, Wyoming	ANNA G. ESHOO, California
JOHN SHIMKUS, Illinois	BART STUPAK, Michigan
HEATHER WILSON, New Mexico	ELIOT L. ENGEL, New York
JOHN B. SHADEGG, Arizona	ALBERT R. WYNN, Maryland
CHARLES W. "CHIP" PICKERING, Mississippi	GENE GREEN, Texas
VITO FOSSELLA, New York	KAREN McCARTHY, Missouri
ROY BLUNT, Missouri	TED STRICKLAND, Ohio
STEVE BUYER, Indiana	DIANA DeGETTE, Colorado
GEORGE RADANOVICH, California	LOIS CAPPAS, California
CHARLES F. BASS, New Hampshire	MICHAEL F. DOYLE, Pennsylvania
JOSEPH R. PITTS, Pennsylvania	CHRISTOPHER JOHN, Louisiana
MARY BONO, California	TOM ALLEN, Maine
GREG WALDEN, Oregon	JIM DAVIS, Florida
LEE TERRY, Nebraska	JAN SCHAKOWSKY, Illinois
ERNIE FLETCHER, Kentucky	HILDA L. SOLIS, California
MIKE FERGUSON, New Jersey	
MIKE ROGERS, Michigan	
DARRELL E. ISSA, California	
C.L. "BUTCH" OTTER, Idaho	

DAN R. BROUILLETTE, *Staff Director*

JAMES D. BARNETTE, *General Counsel*

REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida	EDWARD J. MARKEY, Massachusetts
JOE BARTON, Texas	<i>Ranking Member</i>
CLIFF STEARNS, Florida	BOBBY L. RUSH, Illinois
<i>Vice Chairman</i>	KAREN McCARTHY, Missouri
PAUL E. GILLMOR, Ohio	MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER COX, California	JIM DAVIS, Florida
NATHAN DEAL, Georgia	RICK BOUCHER, Virginia
ED WHITFIELD, Kentucky	EDOLPHUS TOWNS, New York
BARBARA CUBIN, Wyoming	BART GORDON, Tennessee
JOHN SHIMKUS, Illinois	PETER DEUTSCH, Florida
HEATHER WILSON, New Mexico	ANNA G. ESHOO, California
CHARLES W. "CHIP" PICKERING, Mississippi	BART STUPAK, Michigan
VITO FOSSELLA, New York	ELIOT L. ENGEL, New York
CHARLES F. BASS, New Hampshire	ALBERT R. WYNN, Maryland
MARY BONO, California	GENE GREEN, Texas
GREG WALDEN, Oregon	JOHN D. DINGELL, Michigan,
LEE TERRY, Nebraska	(Ex Officio)
W.J. "BILLY" TAUZIN, Louisiana	
(Ex Officio)	

CONTENTS

	Page
Testimony of:	
Hancock, William, Chief Executive Officer, Internet Security Alliance	30
Holleyman, Robert W., II, President and Chief Executive Officer, Business Software Alliance	42
Pethia, Richard D., Director, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University	13
Silva, Ken, Vice President, VeriSign Inc	26
Wong, Arthur, Vice President, Security Response, Symantec Corporation .	37

COMPUTER VIRUSES: THE DISEASE, THE DETECTION, AND THE PRESCRIPTION FOR PROTECTION

THURSDAY, NOVEMBER 6, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON TELECOMMUNICATIONS
AND THE INTERNET,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2123, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Stearns, Deal, Shimkus, Bass, Bono, Walden, Markey, McCarthy, Eshoo, and Green.

Staff present: Kelly Zerzan, majority counsel; Will Nordwind, majority counsel and policy coordinator; Neil Fried, majority counsel; Jaylyn Connaughton, majority professional staff; Will Carty, legislative clerk; Peter Filon, minority counsel; and Jessica McNiece, minority research assistant.

Mr. UPTON. Good morning, everyone. I apologize for this virus, but I would rather have this virus than one at my house on my computer. You need to take that sucker back to the hospital.

Good morning. Today's hearing is entitled "Computer Viruses: The Disease, the Detection and the Prescription for Prevention." If someone had told me a few years ago that an evil scientist plotted from his underground lair to send a malicious code to infect computers all around the world with a worm which would first replicate itself for the first 20 days of each month, the second would deploy web pages on infected servers with a page that declared "hacked by the Chinese" and third launch a concerted attack on the White House Web server in an attempt to overwhelm it, I would have guessed that this was the latest plot in the next James bond movie. What we now know is, in fact, this happened with the "Code Red" worm in July 2001.

Unfortunately, worms and viruses are not science fiction. They are an alarming fact of life in the Internet age. The Internet now connects over 170 million computers, and the number continues to grow. Our society is increasingly dependent upon the Internet to communicate bank and purchase goods and services. Moreover, many of our Nation's important functions, such as the electricity grid, the stock exchanges, the banking system and commerce rely in large part on the smooth and uninterrupted operation of the Internet.

Without a doubt, our reliance on the Internet has had a positive effect on the productivity, efficiency and convenience of our country. However, it is precisely this fact which makes us so vulnerable to the havoc which can be wreaked by viruses and worms. I speak from experience when I say that anyone who has lost files or work or has had their computer crash due to a worm or virus knows the frustration which they cause.

In addition, worms and viruses can cause tremendous economic damage. So far, damages in the form of lost productivity, wasted hours, lost sales, extra bandwidth from the "Blaster" worm alone are estimated to be at least \$525 million; and "Sobig.F" damages are estimated to be over \$500 million again. Some estimates are even higher, even in the billions of dollars.

As bad as that is, in the wake of September 11, there is the even more chilling specter of cyberterrorist attacks on our Nation's increasingly Internet-dependent critical infrastructures. Research and analysis suggests that worms and viruses are proliferating and are able to move with increasing speed across the globe. According to testimony we are going to hear today, the "Slammer" worm had a significant impact in just minutes; and the depressing fact is that it only takes one personal computer, some decent programming skills, a warped mind and a cruel heart to launch a virus or a worm with over 40,000 viruses and their variant strains that have been identified to this day. It appears as if these traits are not in short supply.

Law enforcement is a critical element in stopping those who seek to infect the Internet with viruses and worms, and I would note that just yesterday Microsoft announced that it has put up \$5 million in reward money for information which will lead law enforcement to the successful capture of the culprits who launch destructive viruses and worms. I applaud their efforts.

While I hope that the bounty will help, I recognize that law enforcement in this area is extremely challenging. That is why the focus of today's hearing is on the prescription for protection. We need to figure out how both we can adequately arm all levels of government, business and the consumers with the best information as to what steps they can take to protect themselves and how we can ensure that everyone takes those steps. That is what we hope to learn today from the distinguished panel.

At this point I yield to the ranking member of the subcommittee, my friend the, gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman.

Did you say you had a virus, Mr. Chairman?

Mr. UPTON. Yeah. Is that why you are over there?

Mr. MARKEY. Yeah. So—

Mr. UPTON. I haven't touched the documents over here yet, so it is spreading throughout the office just like that. I have got two people sick today—one yesterday, three today.

Mr. MARKEY. So—

Mr. UPTON. Congress will be out of session tomorrow for good reason.

Mr. MARKEY. And a real virus—what you have is much worse than anything these people are going to talk about. I mean infinitely worse, okay? So just so we can—if we can have a hearing on

a computer virus, then we should actually try to take measures—they are going to tell us about how to prevent the spread of these viruses, right? So I am going to try to stay over here.

Mr. UPTON. There is no feeder.

Mr. MARKEY. And I want to commend you for calling this hearing. It is a subject that plagues millions of computer users as well as businesses around the country. They can wreak havoc as they propagate their way through computer networks, including the Internet. Because of the increasing interconnectedness of our Nation's telecommunications and computer infrastructure and the fact that ever more Americans go on-line every year, we can see an increased vulnerability to the debilitating nature of a virus attack.

There are some 65,000 viruses for the Windows program, which over 90 percent of American computer users utilize. Some computer experts have pointed out the inherent vulnerability of millions of computer users relying upon the same operating system. The very interoperability and efficiency that businesses and computers prize about their telecommunications and computer capabilities have an Achilles-heel quality if preyed upon by computer programmers with nefarious intent.

Microsoft has announced recently a program to make bounty payments to those who lead them to the creators of viruses that attack Microsoft software. The result of a cyberattack can cause consumers to lose valuable files and data. They can render a computer network inoperable for hours or even days, and they can cost victims millions of dollars in lost time, sales and equipment.

A whole industry has grown up with the personal computer to help thwart such attacks and fight viruses. Much like in the real world, where new viruses or variations of older strains may arise each flu season requiring new vaccination, software programmers for security firms are constantly battling new viruses that are launched onto the Internet on a seemingly daily basis. One estimate indicates that U.S. companies spent over \$12 billion last year alone in combatting and cleaning up after virus attacks.

Moreover, with the threat posed by terrorists, especially intelligent, sophisticated terrorist organizations with access to great financial resources, the prospect of cyberterrorism is a clear danger to our key infrastructure and our economy.

I want to commend you, Mr. Chairman, for calling this timely hearing; and I yield back the balance of my time.

Mr. UPTON. Thank you, Mr. Markey. Mr. Shimkus from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. I also want to thank you for holding this hearing.

I do have a bill that is being marked up in the Senate Foreign Relations Committee this morning. I am going to run over there and do some personal lobbying on that. I am really the last person that wants to make any analysis or comment on security at this time, so I respectfully yield back the balance of my time.

Mr. UPTON. Make sure you have an escort over to the Senate.

Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman, for calling this hearing regarding impacts and solutions for the computer virus problem.

Computer viruses are causing terrible harm to the computer users and billions in damages to U.S. Businesses. Computer tech-

nologies have delivered tremendous benefits to our economy and society in the recent years, but there are unintended consequences. We have unsolicited e-mails, we have viruses, we have computer worms, and recent combinations of that are attempting to swarm our networks. The combination of e-mail, spam and viruses is like putting a SARS patient on every airline flight in the country.

In August, the Sobig virus became the fastest-spreading and most pervasive computer virus in history. How did Sobig spread so fast? Spam. What was the cost? At least \$3 billion.

An August 12, 2003, Business Week article described how virus writers and spammers are borrowing each others techniques with devastating consequences; and, Mr. Chairman, I ask unanimous consent to place this Business Week article in the record.

Mr. UPTON. Without objection.
[The article follows:]

SECURITY NET

By Jane Black

UNHOLY MATRIMONY: SPAM AND VIRUS

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 log-on 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. A third even more despicable tactic is also a possibility, a spam message with a virus that turns innocent computers into senders of more spam. It is the invasion of the in-box snatchers, with spammers turning our computers into spamming zombies with virus-infected spam infecting our networks.

I am glad we are having this hearing to see what private-sector solutions can be developed to attack this new and mutated infection. But there is also something this committee and this Congress can do about it. To complement and support private-sector efforts to stop spam and spam viruses, the majority of members of our committee are sponsors of H.R. 2515, the Wilson-Green Anti-Spam Act of 2003, which is the strongest anti-spam bill in Congress.

Many are impressed that the Senate acted so quickly on their spam legislation, but I want to warn my colleagues that a weak spam bill will be worse than none at all. If we are going to preempt State laws under which State actions are currently being brought, it needs to be a strong Federal law. With the unholy alliance of spam and viruses we need all the law enforcement tools on hand to protect ourselves.

The Senate-passed bill has ineffective enforcement, as a bipartisan Internet committee of the National Association of Attorney Generals concluded in their November 4 letter. The letter was signed by the Texas Attorney General, along with Attorney Generals from California, Kansas, Maryland, Nevada, Vermont, Virginia and Washington. And, again, Mr. Chairman, I ask unanimous consent to enter this into the record.

Mr. UPTON. Without objection.

[The information referred to 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)(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).

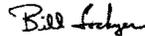
10. Section 108(b) preempts many state laws which regulate the use of electronic mail. Though states' statutes prohibiting falsity or deception in commercial email are not preempted, numerous states have taken a broader approach to regulation. Some states require labeling, others provide for specific 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,



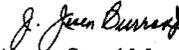
Attorney General Christine O. Gregoire
Attorney General of Washington
Chair, NAAG Internet Committee



Attorney General Bill Lockyer
Attorney General of California
NAAG Internet Committee



Attorney General Phil Kline
Attorney General of Kansas
NAAG Internet Committee



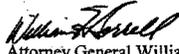
Attorney General J. Joseph Curran Jr.
Attorney General of Maryland
NAAG Internet Committee



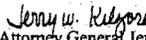
Attorney General Brian Sandoval
Attorney General of Nevada
NAAG Internet Committee



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. Gilmor
 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
 Chris Cannon
 Spencer Bachus
 John N. Hostettler
 Mark Green
 Ric Keller
 Melissa A. Hart
 Jeff Flake
 Mike Pence
 Randy Forbes
 Steve King
 John R. Carter
 Tom Feeney
 Marsha Blackburn

Howard L. Berman
 Rick Boucher
 Jerrold Nadler
 Bobby Scott
 Melvin L. Watt
 Zoe Lofgren
 Sheila Jackson Lee
 Maxine Waters
 Marty Meehan
 William Delahunt
 Robert I. Wexler
 Tammy Baldwin
 Anthony D. Weiner
 Adam Schiff
 Linda T. Sánchez

Mr. GREEN. To cite one example of how strong anti-spam legislation will cut down on computer viruses, the Wilson-Green bill bans misleading subject lines. Misleading subject lines are a primary way that spam viruses work, enticing innocent users to open dangerous e-mail.

The bill offered by my good friend, Mr. Burr of North Carolina, does not prohibit misleading subject lines. The bill that passed the Senate allows spammers an affirmative defense clause so that they can argue that they tried to follow a law while they were actually violating it.

The Wilson-Green bill also prohibits dictionary attacks, a highly effective spamming method that can make a spam virus even more devastating. Neither the Burr bill nor the Senate-passed bill prohibits dictionary attacks.

These differences don't just impact how much consumers are annoyed. They have a major impact on our economy. I stand ready to continue working with the Chairman of the subcommittee, the full committee and Mr. Burr to get a strong bill out to the House.

In closing, I want to mention again that just one spam virus caused at least \$3 billion in economic damages. Some estimates are much higher. Viruses used to be sent out by hackers trying to prove how smart they are. Now spam viruses like Sobig are being sent out by people trying to see how much money they can make. I believe we need to act on a strong anti-spam legislation with law enforcement that is tough as soon as possible.

Again, Mr. Chairman, thank you for holding this hearing; and again, to this distinguished panel, I look forward to their responses. Thank you.

Mr. UPTON. Thank you very much.

Mr. Walden.

Mr. WALDEN. Thank you, Mr. Chairman. I am going to defer an opening statement.

I just hope we can figure out how to get these modern-day vandals early and prevent this kind of abuse. I look forward to the testimony of the panel. I intend to read their submitted testimony.

Thank you, Mr. Chairman.

Mr. UPTON. Thank you very much.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. PAUL E. GILLMOR, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF OHIO

I thank the Chairman for the opportunity to address this important issue. The increasing use of computers and the steady spread of the digital age continues its worldwide impact. Yet, the negative effects of computer viruses threaten our personal and national security.

Each day, thousands of people and corporations find their computer infrastructure compromised by viruses, worms, and other digital threats. In 2002, computer viruses in the United States caused nearly \$50 million in damages. The August 2003, threat of the Sobig and virus alone cost almost \$30 billion in worldwide damages.

Today we are a nation dependent on the resources of the digital age. The use of the Internet, email, instant messaging, and online shopping and banking provide many Americans with the resources for a simpler life. However, the many wonderful features of computers and the Internet are often overshadowed by the acts of the malicious few. The 50 percent increase in theft of confidential data during the first half of this year is just one of the many evils that will continue to face our people and businesses.

In addition, we face an imminent threat to our national security systems which cannot be ignored. The reliance on digital technology by the energy, medical and de-

fense systems across the United States and my State of Ohio, while necessary, leaves our country susceptible to many dangers. The lack of solid computer security measures capable of protecting against a constant bombardment of technology attacks poses a direct threat to our national security.

Our first priority has to be informing the people. As a first step, an increased use of anti-virus software and firewalls will assist in securing many of the computers and systems currently vulnerable to attack. All of our friends, families, and staffs have felt the effects of digital attacks; some through personal trauma, others through the press, but all through the damaging results on our country and our economy. Today we must commit to inform and assist in this fight.

I welcome the well-balanced panel of witnesses and look forward to hearing your perspectives concerning this timely issue.

Again, I thank the Chairman and yield back the remainder of my time.

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS
FROM THE STATE OF WYOMING

Thank you, Mr. Chairman.

I would like to thank you for holding this hearing to examine the scourge of computer viruses. As our nation continues its evolution to a fully wired or in this day and age Awireless@ technological society, the impact of malicious computer programs can be staggering. Frankly, it's hard for me to comprehend why someone would consciously act to debilitate the property of others. Just as puzzling as the brazen acts of thieves and other common thugs, or the international threat of homicide bombings, the proliferation and complexity of these cyberattacks are testaments to the growing criminal element and national security threat that worms and viruses embody.

As a result of this hearing I would like to get a better understanding of the scope of the problem and the impact it has on commerce and the operation of our nation's electronic infrastructure. I am also hoping that our expert panel can clarify the differences between worms and viruses and explain what steps consumers and businesses can take to inoculate themselves against vulnerability. I'm also curious what role Congress plays in this matter. After all, it strikes me as a difficult endeavor in the anonymous realm of the Internet to catch the perpetrators of these crimes, while simultaneously observing constitutional protections against search and seizure.

Nevertheless, as a Member representing rural Wyoming, where the Internet keeps us connected to the rest of America, I have concerns about how these vulnerabilities affect the small businesses and entrepreneurs across the state, and by extension our local economy.

We have the opportunity in today's hearing to fully analyze the threat of worms and viruses and make certain that not only is our marketplace secure but also the vital government computer systems that could be tempting targets for a terrorist attack.

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

PREPARED STATEMENT OF HON. MARY BONO, A REPRESENTATIVE IN CONGRESS FROM
THE STATE OF CALIFORNIA

Mr. Chairman, I would like to thank you for your leadership on this issue. Computer viruses and worms pose a substantial threat to the Internet, consumers, and the stability of businesses. I look forward to hearing from the witnesses to learn more about various ways we may help in the fight against cyber attacks.

It is unfortunate that some have found ways to program malicious code onto the computers of others. Such codes substantially slow down computer performance and sometimes even bring computers to a screeching halt.

The result is more than mere inconvenience. Such security violations are quite costly. In fact, experts estimate that corporations in the United States alone spent approximately \$12.3 billion to clean up damage from computer viruses in 2001, and that the worms of this past summer costs businesses up to \$3 billion.

Part of the problem is that often times, the potential damage is undetectable until it is too late. Businesses as well as consumers are repeatedly uninformed about possible cyber attacks. In fact, some cyber attacks can be launched, while remaining entirely undetectable.

For example, as many of you know, this past July, I along with Congressman Edolphus Towns, introduced H.R. 2929, "the Safeguards Against Privacy Invasions Act," or rather the SPI Act. This bill aims to address the issues related to

“spyware.” Like viruses, spyware programs embed codes into other computer programs, affecting the efficiency of computers.

However, spyware is even more threatening since such code can be used to actually spy on computer users. Some spyware programs track the actions of Internet travelers for the purpose of presenting targeted advertisements, but many spyware programs are used to view computer users’ actions, enabling access to personal and financial information by unknown entities.

According to a recent industry publication, spyware is rampant and problematic, and “nearly 75 percent of customer problems with computer performance can be linked in some way to spyware and its applications.” *The Reporter* (July 7, 2003). Despite this enormous effect on computer users, shortly after introducing the SPI Act, it became evident to me that many members of Congress and consumers are unaware of spyware.

I hope to hear the witnesses’ thoughts on the issue of spyware as it relates to computer viruses and other computer problems, and I urge my colleagues to seriously consider this issue, as I feel that it may be one of the most serious threats facing our computer-using constituents.

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

Thank you, Mr. Chairman, for holding this very important hearing today on computer worms and viruses. We saw a summer season full of news stories about computer bugs with names such as “Blaster” and “Slammer,” and I hope this hearing can shed some light on this very troubling subject.

There is no question that modern computer viruses are the “common cold” of the Internet. They can spread quickly across open networks, like the Internet, and each bug can cause billions of dollars in damage in its wake.

To put the threat into some perspective, five years ago the chance of receiving a virus over a 12-month period was about 1 in 1000. Today, the chance of infection has dropped dramatically to about 1 in 10. In fact, while the number of Internet users continues to grow at a healthy pace, the dangerous activity on the Internet is growing even faster.

Virus experts have recorded more than 65,000 worms and viruses and their strains over the years. Although, thankfully, most viruses are annoying time-wasters. Increasingly, however, we are seeing more advanced and sophisticated threats that can deliver a destructive payload.

Traditionally, we have viewed cyber attacks as threats to information that could wreak havoc on businesses, governments and economies across the world. But today, our nation’s critical physical infrastructure is powered by computer systems that utilize the Internet. Such attacks can shut down facilities like airports, bridges, electrical grids, nuclear plants, and air traffic control—posing enormous public safety risks. It is only a matter of time before Internet worms and viruses are used to attack infrastructure that will result in more than just financial losses. For this reason, cyber security must be at the forefront of the minds of those in business and government.

We have an excellent panel of experts before us today to educate us on this important issue. Businesses need to ramp up their cyber security, consumers need to be vigilant, and Congress must continue to ensure our computer and technology networks are safe.

I am anxious to hear from our witnesses what can be done to stem the tide of computer worms and viruses, what steps are being taken to address our vulnerabilities, and what role, if any, the federal government—specifically the Congress—can play to promote increased awareness and action on these issues.

Thank you again, Mr. Chairman for holding this hearing. I yield back my time.

PREPARED STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, thank you for holding this hearing.

I’d like to welcome Ken Silva of VeriSign and Art Wong of Symantec. Both VeriSign and Symantec are based in my district and I’m proud that they join this panel of experts today to discuss what I think could be one of the most important hearings this panel holds.

Our country is increasingly dependent on the network of computers that make up the Internet.

We use this technology in our day-to-day activities...from checking the weather to our checking account.

Most people don't realize the amount of personal information readily available through the Internet and how vulnerable this information is to cyber attacks and how fragile our patchwork of networked critical infrastructure really is.

The blackout in the Northeast last August is an example not only of how connected we are, but how, when parts of those connections fail, entire regions and sectors of our economy can literally be shut down.

Clearly the protection of this infrastructure is an important topic that the Congress must address.

The number of worms and computer viruses that have paralyzed the Internet and seriously affected our economy have grown in the last year.

This is not just hacking taking place—these worms and viruses can stop the commerce taking place over the Internet. There are severe economic consequences to these cyber attacks. It's calculated that the worm attacks this summer cost nearly \$2 billion dollars.

Our ability to respond to these threats greatly depends on cooperation between the public, the private sector and the federal government. The Department of Homeland Security is one of the key components in establishing a relationship with the private sector that will help build programs to combat these threats. There's much work to be done, but we've at least begun to address the serious threat of cyber attacks through homeland security initiatives.

We also need to make sure that we promote consumer education and awareness of these threats.

Individual home users need to realize that their Internet use is also vulnerable to attacks and their computers may be used to disseminate computer viruses.

Mr. Chairman, thank you for holding this important hearing. I look forward to the testimony of our panel of experts and working with you to solve this national challenge.

Mr. UPTON. Well, we are delighted to have a distinguished panel this morning. We are honored to have Mr. Richard Pethia, the Director of the CERT Coordination Center from the Software Engineering Institute; Mr. Ken Silva, Vice President of VeriSign; Dr. Bill Hancock, Chief Executive Officer of Internet Security Alliance; Mr. Art Wong, Vice President of Security Response for Symantec Corporation; and Mr. Robert Holleyman II, President and CEO of Business Software Alliance here in Washington.

Gentlemen, your statements are made part of the record. At this point we would like you to take 5 minutes each to give an opening statement, at which point, when you are finished, we will have questions from the members that are here.

Mr. Pethia.

STATEMENTS OF RICHARD D. PETHIA, DIRECTOR, CERT COORDINATION CENTER, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY; KEN SILVA, VICE PRESIDENT, VERISIGN INC.; WILLIAM HANCOCK, CHIEF EXECUTIVE OFFICER, INTERNET SECURITY ALLIANCE; ARTHUR WONG, VICE PRESIDENT, SECURITY RESPONSE, SYMANTEC CORPORATION; AND ROBERT W. HOLLEYMAN, II, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BUSINESS SOFTWARE ALLIANCE

Mr. PETHIA. Thank you, Mr. Chairman and members of the subcommittee, for the opportunity to talk to you today about the important issue of cyberviruses and worms. My views today are shaped by the lessons we have learned at the CERT Coordination Center where for 15 years we have dealt with the problem and more recently have partnered with the Department of Homeland Security to form the U.S. CERT.

Today, worms and viruses are a growing risk that cause damage more quickly than those created in the past. With the Code Red worm in 2001, there were days between the first identification and the widespread damage. In January of this year, Slammer had significant impact in just minutes.

As already mentioned this morning, virus and worm attacks alone have resulted in millions of dollars of damage, with individual viruses often causing damage in excess of \$500 million. While the viruses and worms we have seen in the past have infected computers, clogged networks and mail servers, few have been programmed to do more than just propagate. In the future, it is likely we will see viruses and worms carrying payloads that delete or corrupt data and program files or leak sensitive information.

It is clear that our current reactive solutions alone are no longer adequate. With the Internet now connecting over 171 million computers and with many attacks now being fully automated, they spread with blinding speed across the entire Internet community. The attack technology is becoming increasingly complex, increasing the time it takes to analyze the attack mechanisms in order to produce antidotes. With increasing dependency on the Internet even short interruptions of service can cause significant economic loss in very short periods of time.

What can we do?

First of all, we need to continue to improve our warning and response capabilities by building collaborative partnerships across organizations that participate in cyberwatch warning and response functions.

Second step is to reduce vulnerabilities by collaborating with the private sector to develop new tools and methods for detecting and remediating vulnerabilities in products that are commonly used in our information infrastructures. Especially needed are new generations of software that are virus resistant or virus proof. Vendors need to provide systems and software that constrain the execution of imported code, especially the code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as sandbox attack techniques, are more recent.

We need to dramatically reduce implementation errors. Last year over 4,000 new vulnerabilities were reported to the CERT Coordination Center.

While it is unlikely that we will ever be able to develop defect-free software, vendors need to be proactive, study and learn from past vulnerabilities and adopt new known, effective software engineering practices that dramatically reduce the number of flaws in their software products.

Finally, we need high security default configurations, out-of-the-box software configurations that have security options turned on, rather than depending on the users to turn them on.

System operators also need to take critical systems to adopt security practices. Senior managers must visibly endorse security improvement efforts and support adoption of effective practices and technologies and provide the resources needed to implement those improvements, keeping their skills and knowledge current by at-

tending courses and using information sources that continue to track this dynamic and ever-changing problem.

Finally, home users must improve their understanding of the problems and use practices and technology such as anti-virus products and personal computer firewalls.

Other things we think the government can do would be to provide incentives for higher quality, more secure products. The government should use its buying power and adopt code integrity clauses, clauses that hold the vendors more accountable for security defects and provide incentives for vendors to supply low-defect products and products that are highly resistant to viruses.

Also in this area are upgraded acquisition processes that put more emphasis on the security characteristics of the systems being required.

In the long term, research is needed to develop a unified and integrated framework for all information assurance analysis design and implementation, rigorous methods to assess and manage risks, and simulation tools to analyze the possible cascade effects of attacks across interdependent systems.

The government scholarship programs that currently exist to produce security specialists are doing a good job, but we need to expand those programs over the next 5 years to build the university infrastructure we will need for the long term.

Finally, we need more awareness and training for all Internet users, including the development of educational material for children in the K through 12 age frames.

The National Cybersecurity Division formed by the Department of Homeland Security and the U.S. CERT are steps toward implementation of these recommendations, but a safer cyberspace will require that the NCSA, the entire Federal Government, State and local governments and the private sector all work together to improve security practices, create higher quality software, build awareness at all levels and sponsor increased research and development activities leading to new generations of virus-tolerant products.

[The prepared statement of Richard D. Pethia follows:]

PREPARED STATEMENT OF RICHARD D. PETHIA, DIRECTOR, CERT® COORDINATION CENTER, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

INTRODUCTION

Mr. Chairman and Members of the Subcommittee: My name is Rich Pethia. I am the director of the CERT® Coordination Center (CERT/CC). Thank you for the opportunity to testify on the important issue of cyber security. Today I will discuss viruses and worms and the steps we must take to protect our systems from them.

The CERT/CC was formed in 1988 as a direct result of the first Internet worm. It was the first computer security incident to make headline news, serving as a wake-up call for network security. In response, the CERT/CC was established by the Defense Advanced Research Projects Agency at Carnegie Mellon University's Software Engineering Institute, in Pittsburgh with a mission to serve as a focal point to help resolve computer security incidents and vulnerabilities, to help others establish incident response capabilities, and to raise awareness of computer security issues and help people understand the steps they need to take to better protect their systems. We activated the center in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled 260,000 incidents, cataloged and worked on resolutions to more than 11,000 computer vulnerabilities, and published hundreds of security alerts.

In September of this year, the Department of Homeland Security, in conjunction with Carnegie Mellon University, created the US-CERT. The US-CERT is a growing partnership between the CERT/CC and DHS's National Cyber Security Division (NCSA) and is forging strong partnerships with many different types of organizations that conduct cyber security analysis and response efforts—From government laboratories, to academic institutions, to major hardware and software suppliers. The US-CERT is focused on preventing and mitigating cyber attacks and reducing cyber vulnerabilities. It provides the needed focal point for these over two hundred private, public, and academic organizations that conduct cyber security incident watch, warning, response, and prevention functions.

GROWING RISK FROM WORMS AND VIRUSES

Worms and viruses are in a more general category of programs called “malicious code.” Both exploit weaknesses in computer software, replicating themselves and/or attaching themselves to other programs. They spread quickly and easily from system to system. By definition, worms are programs that spread with no human intervention after they are started. Viruses are programs that require some action on the part of the user, such as opening an email attachment, before they spread. Users are often enticed to open email attachments, sometimes because of an intriguing or legitimate-sounding subject line and sometimes, when address books have been compromised, because the email appears to be from someone the user knows. Worms and viruses can bypass security measures, such as firewalls, and clog systems to the point that response is slow or shut off.

Today, worms and viruses are causing damage more quickly than those created in the past and are spreading to the most vulnerable of all systems—The computer systems of home users. The Code Red worm spread around the world faster in 2001 than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. Just months later, the Nimda worm caused serious damage within an hour of the first report of infection. In January of this year, Slammer had significant impact in just minutes.

The figures attached to the end of this testimony show the speed and magnitude of the Blaster worm compared to previous worms, as well as indications of Blaster's and Sobig.F's continued impact. Figure 1, *Blaster, Slammer, and Code Red Growth Over Day 1*, shows how quickly Slammer infected a significant number of computer systems. It shows that Blaster was slightly slower than Slammer, but still much faster than Code Red. After 24 hours, Blaster had infected 336,000 computers; Code Red infected 265,000; and Slammer had infected 55,000. Figure 2, *Comparing Blaster and Code Red in the First 18 Hours*, shows the growth in the number of computers reached by the Blaster and Code Red worms in the first 18 hours. In both cases, 100,000 computers were infected in the first 3 to 5 hours. The fast exploitation limits the time security experts like those at the US-CERT have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

Figure 3, *Blaster-Infected Systems Scanning per Hour: Long-Lasting Effects*, demonstrates how far-reaching worms and viruses can be. After the initial surge of infections from the Blaster worm and subsequent patching, the impact reached a steady-state of 30,000 computers in any given hour. However, it is a different 30,000 computers (an average of 150,000 in any given day), depending on the time of day. Peaks represent activity in different parts of the world, cycling through business days. The Blaster worm is still active and continues to have impacts on computer systems across the globe.

IMPACT OF WORMS AND VIRUSES

At best, worms and viruses can be inconvenient and costly to recover from. At worst, they can be devastating. Virus and worm attacks alone have resulted in millions of dollars of loss in just the last twelve months.

In the 2003 CSI/FBI Computer Crime and Security Survey (www.gocsi.com), viruses were the most cited form of attack (82% of respondents were affected), with an estimated cost of \$27,382,340. The lowest reported cost to a victim was \$40,000, and the highest was \$6,000,000. The Australian Computer Crime and Security Survey found similar results, with 80% of respondents affected by viruses or worms. Of the victims, 57% reported financial losses, totaling \$2,223,900. According to the Australian survey, one-third (33%) of the victims recovered in less than one day, and 30% recovered in one to seven days. The other 37% took more time, including two organizations that believe they might never recover.

So far, damages from the Blaster worm are estimated to be at least \$525 million, and Sobig.F damages are estimated to be over \$500 million (*Business Week*, among other reports in the media). The cost estimates include lost productivity, wasted hours, lost sales, and extra bandwidth costs. *The Economist* (August 23, 2003) estimated that Sobig.F was responsible for one of every 16 email messages that crossed the Internet. In our own experience, Sobig.F has accounted for 87% of all email to our cert@cert.org address from August 18 through the end of that month. We received more than 10,000 infected messages a day, or one message every 8.6 seconds. Figure 4, *Emails messages per Day to cert@cert.org*, shows this in a graph. Sobig.F was so effective because it could send multiple emails at the same time, resulting in thousands of messages a minute. Moreover, Sobig has been refined many times, making it harder to stop (the “F” stands for the 6th version).

IMPLICATIONS FOR THE FUTURE

The significance of our recent experience with Blaster and Sobig.F lies beyond their specific activity. Rather, the worms represent a larger problem with Internet security and forecasts what we can expect in the future.

My most important message today is that the Internet is vulnerable to these types of attack today, and the damage is likely to increase. While the viruses and worms we have seen in the past have caused considerable damage by infecting computers, and clogging networks and mail servers, few have been programmed to do more than just propagate. In the future, it is likely that we will see more malicious attacks with viruses and worms carrying payloads that delete or corrupt data and program files or leak sensitive information. These attacks could easily be aimed at computers used by government organizations at all levels and computers used at research laboratories, in schools, in business, and at home. They are vulnerable to problems that have already been discovered, sometimes years ago, and they are vulnerable to problems that will be discovered in the future.

The implications for Federal, state, and local governments and for critical infrastructure operators is that their computer systems are vulnerable both to attack and to being used to further attacks on others. With more and more government and private sector organizations increasing their dependence on the Internet, our ability to carry on business reliably is at risk.

CURRENT REACTIVE SOLUTIONS ARE LIMITED

For the past 15 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that reactive solutions alone are no longer adequate. To briefly summarize the factors,

- The Internet now connects over 171,000,000 computers and continues to grow at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to one form of attack or another.
- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.
- Many attacks are now fully automated and spread with blinding speed across the entire Internet community, regardless of geographic or national boundaries.
- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.
- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions. Even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions in very short periods of time. Aggressive, coordinated, continually improving response will continue to be necessary, but we must also move quickly to put other solutions in place.

RECOMMENDED ACTIONS—WHAT CAN WE DO?

The actions needed to deal effectively with this growing problem are embodied in the strategy developed by the US-CERT. They include:

- Improved warning and response to incidents with increased coordination of response information
- Reducing vulnerabilities
- Enhancing prevention and protection efforts

IMPROVED WARNING AND RESPONSE

Improved warning and response functions are critically needed to combat fast moving automated attacks such as viruses and worms. To improve current response activities, the US-CERT is building a collaborative partnership between computer security incident response teams, managed security service providers, information technology vendors, security product and service providers and other organizations that participate in cyber watch, warning, and response functions. Working together, and using common information sharing and dissemination principles, the partnership is significantly increasing the nation's ability to protect against and respond to large-scale cyber incidents. Emphasis is currently placed on the development and use of common alerting protocols and collaboration and communication mechanisms to support the rapid identification and analysis of new attacks and the timely production and dissemination and remediation information.

REDUCING VULNERABILITIES

A key component of the US-CERT strategy is to collaborate with the private sector to develop new tools and methods for detecting and remediating vulnerabilities in products commonly used in our information infrastructures. Technology vendors are in a position to help prevent the spread of worms and viruses. Although some companies have begun moving toward improvement in the security in their products, there is a long way to go. Software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. The same types of vulnerabilities continue to appear in newer versions of products that were in earlier versions.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications. These products are complex and often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need. While the current practices allow the user to start using the product quickly and reduce the number of calls to the product vendor's service center when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint. This opens the door to worms and viruses.

It is critical for technology vendors to produce products that are impervious to worms and viruses in the first place. In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- Virus-resistant/virus-proof software. There is nothing intrinsic about computers or software that makes them vulnerable to viruses. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow that code to be executed without constraint on the machine that received it. Unconstrained execution allows program developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.
- Dramatically reducing implementation errors. Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while the products are in use. In many cases, identical flaws are continually reintroduced into new versions of products. The great majority of these vulnerabilities are caused by low level design or implementation (coding) errors. Vendors need to be proactive, study and learn from past mistakes, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- High-security default configurations. With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" con-

figurations if desired, but they would have the benefit of starting from a secure base configuration.

ENHANCING PREVENTION AND PROTECTION EFFORTS

Addressing the threat of worms and viruses is not easy. With approximately 4,000 vulnerabilities being discovered each year, system and network administrators are in a difficult situation. They are challenged with keeping up with all the systems they have and all the patches released for those systems. Patches can be difficult to apply and might even have unexpected side effects. We have found that, after a vendor releases a security patch, it takes a long time for system operators to fix all the vulnerable computer systems. It can be months or years before the patches are implemented on 90-95 percent of the vulnerable computers. For example, the US-CERT still receives reports of outbreaks of the Melissa virus, which exploits vulnerabilities that are more than four years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just given too low a priority. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Moreover, business policies sometimes lead organizations to make suboptimal tradeoffs between business goals and security needs. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

In the face of this difficult situation, the US-CERT is working with the private sector to encourage system operators to take several critical steps.

Adopt security practices: It is critical that organizations, large and small, adopt the use of effective information security risk assessments, management policies, and security practices. While there is often discussion and debate over which particular body of practices might be in some way “best,” it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources.

What is often missing today is management commitment: senior management’s visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

Keep skills and knowledge current. System operators should attend courses that enhance their skills and knowledge, and they should be given the necessary time and support to do so. They need to keep current with attack trends and with tools that help them protect their systems against the attacks. The security problem is dynamic and ever-changing with new attacks and new vulnerabilities appearing daily.

Help educate the users of their systems. System operators must provide security awareness programs to raise users’ awareness of security issues, improve their ability to recognize a problem, instruct them on what to do if they identify a problem, and increase their understanding of what they can do to protect their systems,

RECOMMENDED ACTIONS—WHAT ELSE CAN THE GOVERNMENT DO?

The founding of the National Cyber Security Division and the US-CERT were critical first steps in the US government taking leadership over the cyber security of our nation. Government must continue to show leadership by implementing several key additional actions. These actions include:

Provide incentives for higher quality/more security products. To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include “code integrity” clauses—clauses that hold vendors more accountable for defects, including security defects, in released products and provide incentives for vendors that supply low defect products and products that are highly resistant to viruses. The lower operating costs that come from use of such products should easily pay for the incentive program.

Also needed in this area are upgraded acquisition processes that put more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, acquisition professionals need to be given training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is essential in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

Invest in information assurance research. It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so,

it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the government should support a research agenda that seeks new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

Acquire and foster more technical specialists. Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

Provide more awareness and training for Internet users. The combination of easy access and user-friendly interfaces has drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage “safe computing,” there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one’s own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.¹ Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

The National Cyber Security Division (NCSA), formed by the Department of Homeland Security in June 2003, is a critical step towards implementation of these recommendations. The mission of NCSA and the design of the organization are well-aligned to successfully coordinate implementation of the recommendations that I have described here. However, implementing a “safer-cyberspace” will require, the NCSA and the entire Federal government to work with state and local governments and the private sector to drive better software practices, higher awareness at all levels, increased research and development activities, and increased training for technical specialists.

CONCLUSION

Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple but must be pursued aggressively to allow us to keep our information infrastruc-

¹ National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.

tures operating at acceptable levels of risk. We can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

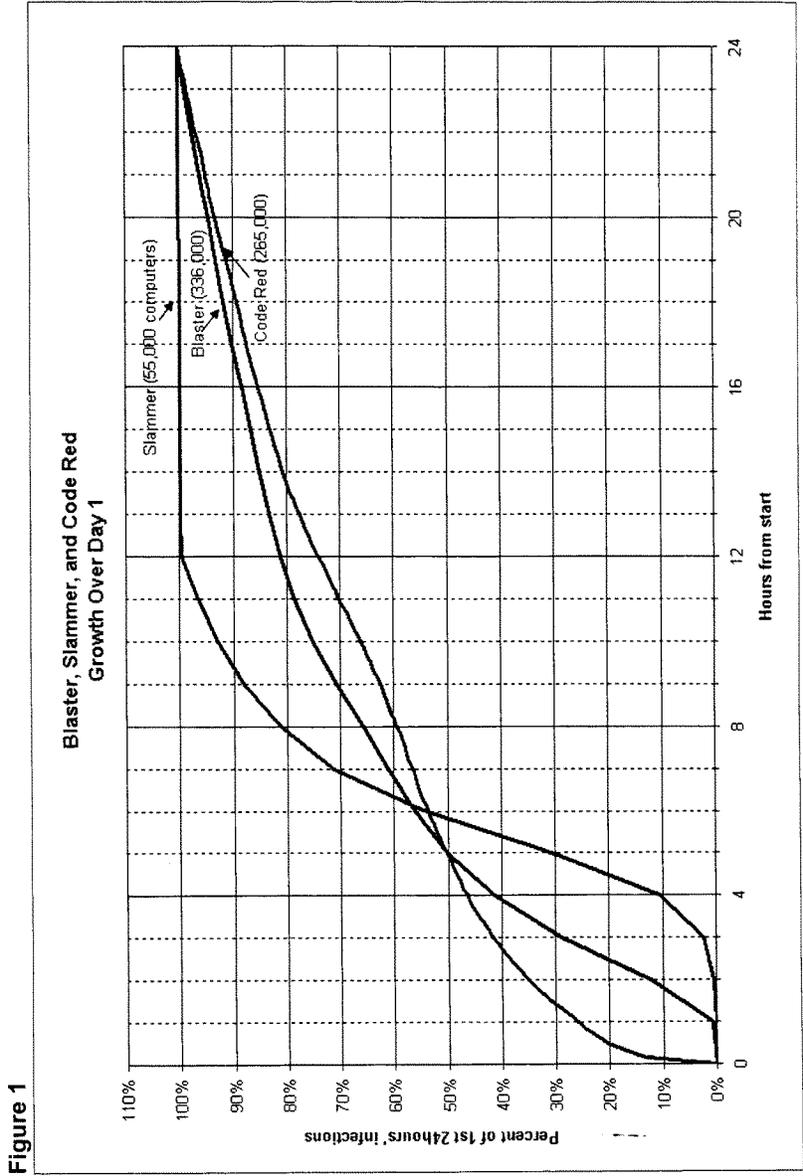
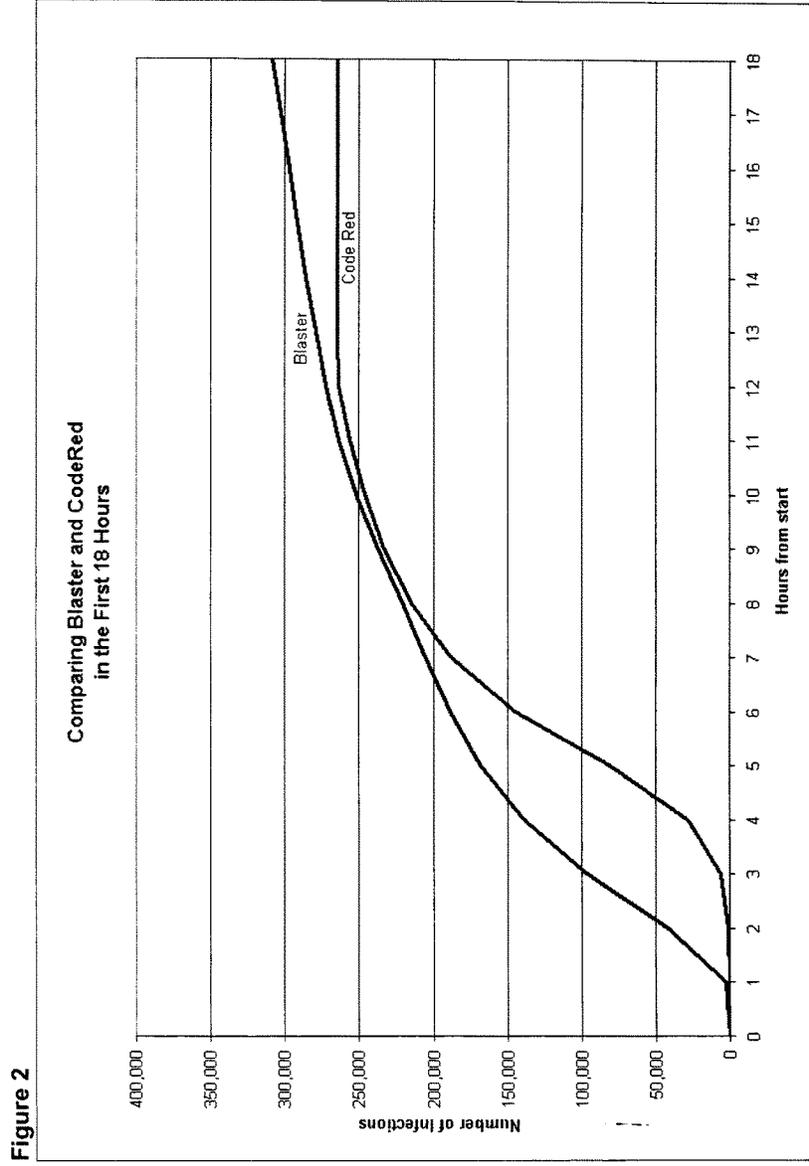


Figure 1



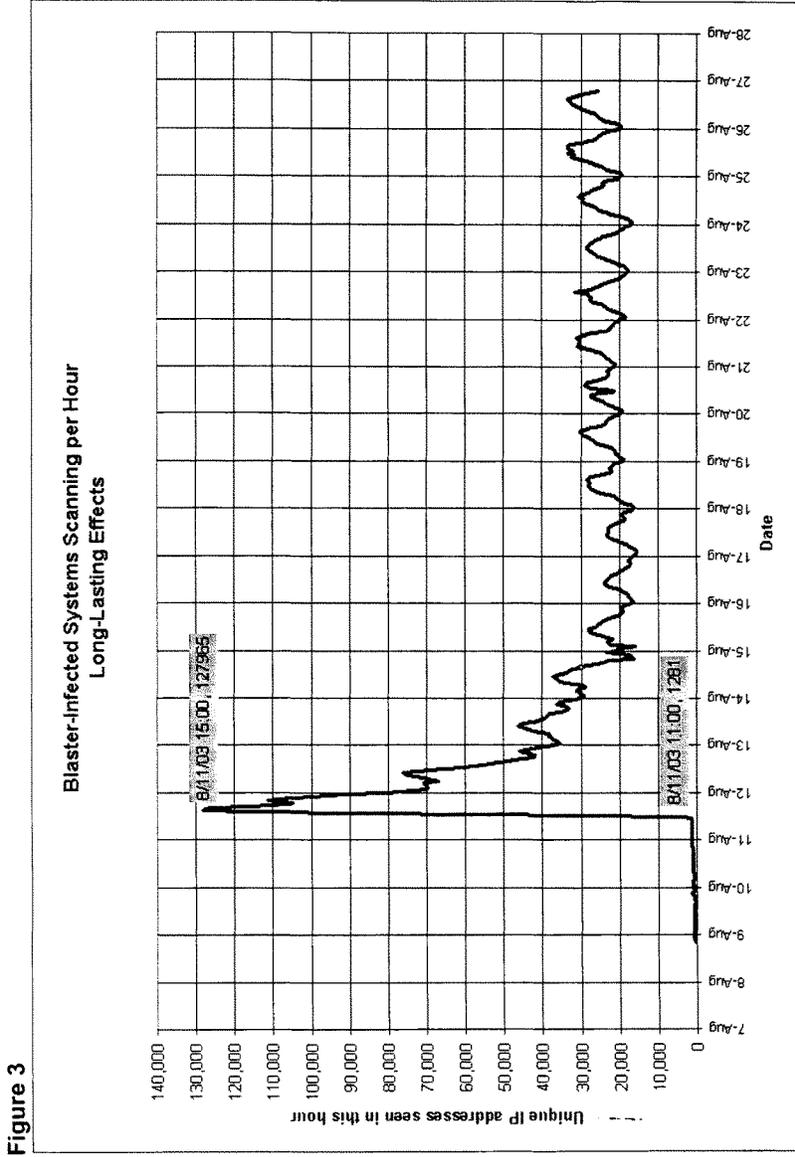
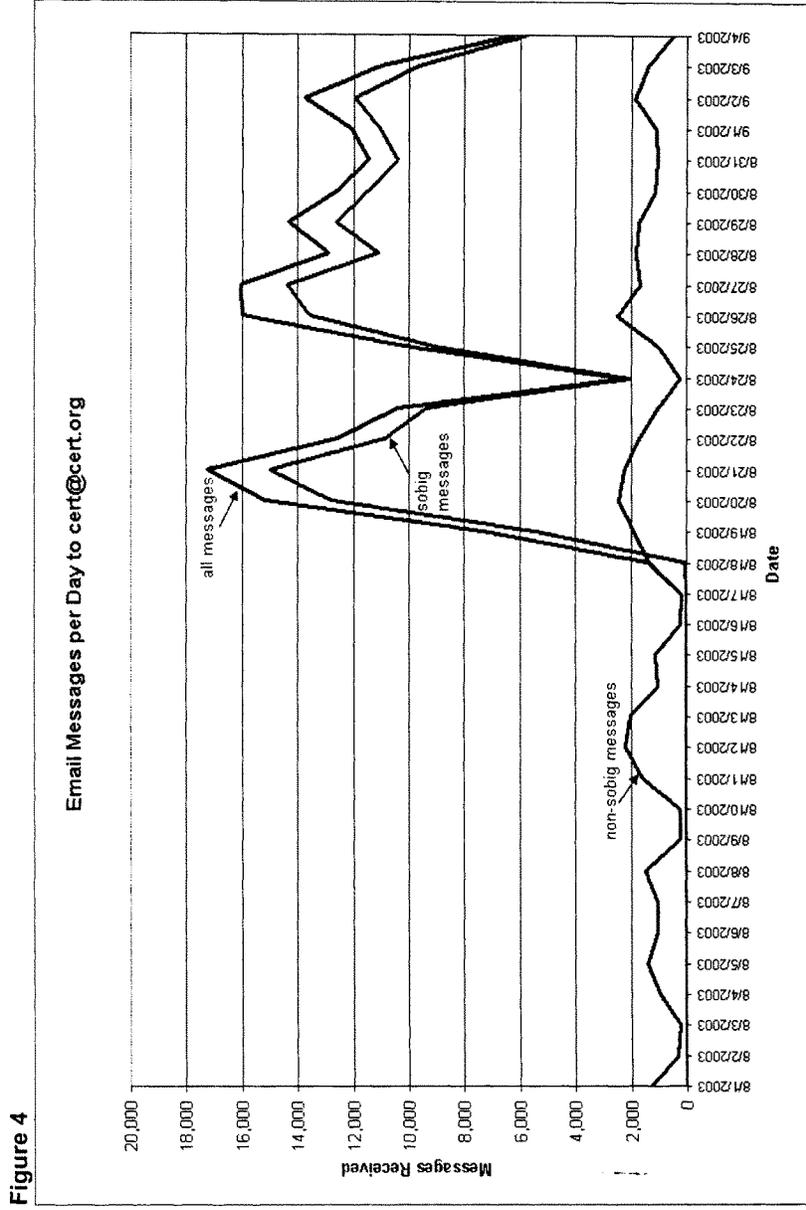


Figure 3



Mr. UPTON. Thank you very much.
Mr. Silva.

STATEMENT OF KENNETH SILVA

Mr. SILVA. Good morning Mr. Chairman, other distinguished members of the subcommittee. We at VeriSign are honored to have the opportunity to provide our views on this very important subject of computer viruses and how we detect their proliferation across the Internet by watching our information networks.

VeriSign is uniquely situated to observe the continuing assaults on our information infrastructure. VeriSign's security organization provides authentication, secure credit card processing, fraud protection, managed security services and a range of other services. Our telecommunications services group provides the essential signaling and switching services to make today's digital telephony, both wired and cellular, possible.

Our naming and directory services includes VeriSign's computer infrastructure dedicated to the management of the Domain Name system of the Internet, including the A and J root servers, the top of the DNS tree.

Since 2000, I have had the privilege of serving both Network Solutions and now VeriSign as manager of the resources dedicated to maintaining security of these complex technology assets.

The proliferation of worms and viruses is costing our Nation's companies billions of dollars. As you have already pointed out this morning, some examples of these costs—and these are just estimates that have been published—Klez, about \$9.5 billion; Love Bug, about \$9 billion; Code Red, \$2 billion; Slammer, \$1 billion; Sobig.F and Blaster combined, somewhere in the neighborhood of \$3.5 billion—and this is just in the month of August alone for Blaster and Sobig. This, coupled with increasingly costly regulatory compliance, is a tremendous burden on our economy and the strength of our industry.

Today, despite widespread perceptions that Internet-related activity has slowed since the bubble burst this March 2000, Internet usage has in fact continued to grow at impressive rates. This is best illustrated by the growth in Internet Domain Name Systems' resolutions. VeriSign's data show that Domain Name resolutions grew by 51 percent year over year between 2002 and 2003. For e-mail alone, that actually grew 245 percent over the same time period. Currently, VeriSign processes over 10 billion Internet Domain Name queries a day on average, which is more than three times what it was in 2000.

This growth in Internet usage has been outpaced, unfortunately, by an increase in security and fraud threats, which are increasing both in number and complexity. The number of security events per device managed by VeriSign's managed security services grew a hundred percent between May and August 2003. From a geographical perspective, the United States continued to be the leading source of these threats to the Internet, accounting for nearly 81 percent of those events.

The Sobig.F e-mail worm, released in August 2003, provides a clear example of the increasing complexity of security threats. This worm was hard-coded to access the Domain Name system root serv-

ers, bypassing the Domain Name servers run by enterprises. As a result, VeriSign recorded a 25fold increase in peak e mail related DNS traffic on its routes when the worm was active.

We are also seeing that Internet fraud is growing rapidly as well. Data from the fraud prevention system indicates that 6.2 percent of e-commerce transactions in the United States were potential fraud attempts. Over 52 percent of those fraud attempts originate from outside of the United States.

There is increasing evidence of overlap between perpetrators of Internet fraud and security attacks. Analysis of the data shows an extremely high correlation, about 47 percent, between sources of fraud and sources of other security-related attacks. Attackers who gain control of Internet host machines are using these compromised hosts for both security attacks and fraudulent e-commerce transactions.

Let me now explain how these three myths in our current state of cybersecurity that must be addressed.

Myth No. 1. The real problem on our networks is not proliferation of worms, virus attacks, identity theft or even spam.

Let me explain this point. The proliferation of worms, viruses, ID theft and spam is not the problem. All of these, while each extremely serious, are only symptoms of a much larger problem that we have today of a highly attractive and vulnerable network across our computer networks.

Myth No. 2. The solution to this problem is to require more rigorous software design to protect individual systems.

Many are tempted to demonize the software vendors and other members of the network community for viruses, worms and attacks. We believe that we must resist this temptation. The idea that somehow if only the operating system vendors made bullet-proof operating systems and applications all Internet security problems would evaporate is purely fiction. The reality is that the weakest link in computer security remains the end users. Many of the worms and viruses take advantage of human behavior and exploit it in order to spread the virus.

Myth No. 3. The objective is a network so secure that it can withstand the evolving and ever more sophisticated assaults.

The point is not to prevent every attack but to make sure that no attack succeeds in bringing down the institution. The point is not to be blindly secure but rather be thoughtfully survivable.

We must stop believing that firewalls, intrusion detection systems and log monitoring alone are adequate security. These are only tools of security. A comprehensive approach that entails those tools, as well as network intelligence on impending or eminent attacks is the only viable solution for success. If we consider this a war on cyberattacks, then we must treat it as such. No military commander would suggest that his troops simply wait in foxholes and return fire when fired upon. They would insist on early warning systems and detailed intelligence about their targets and movements. This is the direction we must head for the war on cyberattacks.

In conclusion, the solutions to our cybersecurity challenge require three commitments.

First, we must provide education to all users to make the investments in hygiene practices and tools necessary and appropriate to their status on the Internet.

Second, we must provide incentives to infrastructure custodians to maintain the investments in research and development to provide the innovative tools that meet the ever-evolving threat of our networks from many sources we have heard about today.

Last, we must provide government at the national and international levels the forensic tools, investigative training, investigative powers and early warning systems.

We believe that these actions will improve the overall health and well-being of the Internet, but none are magic solutions or silver bullets. True long-term health and well-being of our information systems will take time and everyone's efforts. Again, this is as much a responsibility of people as it is technology.

Thank you, Mr. Chairman and members of the committee, for the opportunity to testify before you today.

[The prepared statement of Kenneth Silva follows:]

PREPARED STATEMENT OF KENNETH SILVA, VICE PRESIDENT, NETWORKS AND SECURITY, VERISIGN, INC.

Good morning Mr. Chairman and distinguished members of the Subcommittee. My name is Ken Silva and I am Vice President for Networks and Security of VeriSign, headquartered in Mountain View, California.

We at VeriSign are honored to have the opportunity to provide our views on the very important subject of Computer Viruses and how we detect them proliferating across the internet by watching our information networks.

VeriSign is uniquely situated to observe the continuing assaults on our information infrastructure. Our company provides industry-leading technologies in three relatively distinct—yet interrelated—lines of business. Each of the three serves an important role in the rapidly converging infrastructures that support communication and electronic commerce around the globe.

VeriSign's security organization provides encryption, authentication, secure credit card processing, fraud protection and detection, managed network security services and a range of other services that enable e-commerce, e-government and the overall secure Internet experience that hundreds of millions of users around the globe have come to rely on.

VeriSign's second line of business is our Telecommunications Services group provides the essential signaling and switching services that make today's digital telephony—both wired and cellular—possible. This includes features like call waiting and forwarding, wireless roaming and the soon-to-be available wireless number portability.

Our third major line of business is now known as "naming and directory services," and includes VeriSign's computer infrastructure dedicated to the management of the Domain Name system of the Internet, including our stewardship of the A- and J-root servers—two of the thirteen computers around the globe that represent the top of the pyramid of the Internet's dispersed hierarchy. This is the part of the infrastructure of the Internet that allows each one of you as you type in www.house.gov into your web browser and be instantly connected to one unique computer from among the hundreds of millions on the network. VeriSign also manages the .COM and .NET top-level domains that for many have come to symbolize the essence of the Internet.

Since 2000, I have had the privilege of serving both Network Solutions and now VeriSign as manager of the resources dedicated to maintaining the security of these complex technology assets. On behalf of VeriSign, I also have the privilege of serving in a number of industry leadership capacities, including representing the company on working groups of the President's National Security Telecommunications Advisory Committee—the "NSTAC", working groups of the NRIC, which advises the Federal Communications Commission, and as a board member of both the Internet Security Alliance and the "IT ISAC"—the Information Technology sector's Information Sharing and Analysis Center.

The proliferation of worms and viruses is costing our nation's companies billions of dollars. Some examples of worm costs are; Klez—\$9.5 Billion, Love Bug—\$9 bil-

lion, Code Red—\$2.5 billion, Slammer—\$1 Billion, and Sobig.F and Blaster combined were anywhere from \$3.5-7 Billion in August alone. This coupled with increasingly costly regulatory compliance is a tremendous burden on our economy and the strength of our industry.

In discussing this topic of the proliferation of worms, viruses and hacking attacks, I want to address three key cyber security myths that exist today. But before I discuss these myths, I'd like to begin first with a picture of what we are seeing on the network from our unique perspective as one of the Internet's stewards.

Today, despite widespread perceptions that Internet-related activity has slowed since the "bubble" burst in March 2000, Internet usage has, in fact, continued to grow at impressive rates. This is best illustrated by the growth in Internet Domain Name Systems' resolutions. VeriSign's data show that Domain Name resolutions grew by an average 51% between August 2002 and August 2003. Domain Name resolutions for e-mail grew by 245% in the same time period. Currently, VeriSign processes over 10 billion Internet Domain Name queries a day on average, which is more than 3 times the daily volume in 2000.

This growth in Internet usage has been outpaced by increased security and fraud threats, which increasing both in number and complexity. The number of security events per device managed by VeriSign grew on average by 99% just between May 2003 and August 2003. From a geographical perspective, the United States continued to be the leading source of threats to the internet, accounting for nearly 81% of security events.

The Sobig.F email worm, released in August 2003, provides a clear example of the increase in complexity of security threats. This worm was hard-coded to access the Domain Name System root servers, bypassing the Domain Name servers run by enterprises. As a result, VeriSign recorded a 25-fold increase in peak e-mail related DNS traffic on its roots servers when the worm was active.

We are also seeing that Internet fraud is growing rapidly as well. Data from VeriSign's fraud prevention systems indicate that 6.2% of e-commerce transactions in the United States were potential fraud attempts. Over 52% of fraud attempts originate from outside the United States.

There is increasing evidence of overlap between perpetrators of Internet fraud and security attacks. Analysis of VeriSign's data shows extremely high correlation (47%) between sources of fraud and sources of other security attacks. Attackers who gain control of Internet host machines are using these compromised hosts for both security attacks and fraudulent e-commerce transactions.

Let me now explain how there are three myths in our current state of cyber security that must be addressed.

Myth #1: The real problem on our networks is a proliferation of worms, virus attacks, identity theft or even Spam.

Let me explain this point. The proliferation of worms, viruses, ID theft or even Spam is not *the* problem. All of these—while each extremely serious—are only symptoms of a much larger problem that we have today of a highly attractive vulnerability across our computer networks. Identity thieves, corporate saboteurs, spammers, and mischievous hackers exploit this vulnerability. That vulnerability must be addressed through changed behaviors, both by users and by Internet infrastructure stewards.

Simply put, we all have a shared responsibility as users to uniformly deploy better security hygiene. Whether we are a large e-commerce dependent business or individuals, we can and should do more. At the most basic level, every individual user can contribute to improve security by taking basic steps toward improved security. These prescriptions are well known and widely distributed—yet far too few actually engage even in the most simple, low-cost and no cost measures such as: using passwords and changing them regularly; using anti-virus software and updating it regularly; patching operating systems; getting firewalls and using them; and if you have an always on network connection, turn it off when not using it.

These simple, low cost measures are not a prescription for guaranteed network security. But they are easy steps every user can take to increase their own security posture. By doing so, we improve the overall resilience of the network to attacks. Such measures will strengthen the networks weakest links and those exploited by hackers. When taken, these steps to reduce the population of targeted computers a virus can successfully invade.

MYTH #2: The solution to this problem is to require more rigorous software design to protect individual systems.

Many are tempted today to demonize software vendors and other members of the network community for viruses, worms and attacks. We believe we must resist this

temptation. The idea that somehow if only Microsoft made bulletproof operating systems and applications all Internet security problems would evaporate is purely fiction. This type of finger pointing is often misplaced and in most cases does more harm than good. It is all too simple to blame the operating system manufacturer for flawed code or the network providers for not securing their networks. Many of the worm attack not only popular operating systems, but open source software as well.

This second myth of software user culpability is another area of user responsibility at the consumer and commercial level. This area involves what is called "patch management"—a catch phrase to describe the very important act of maintaining current release levels of software and installing and configuring them appropriately. Only in this way with the benefits of discovered, reported and fixed vulnerabilities that have been addressed through software research and development be put to use on the network.

For the networks stewards such as VeriSign, this area is a crucial aspect of an overall cyber security strategy. Over the past few years in a down economy, we have invested tens of millions of dollars in equipment to provide the massive headroom of servers and storage to withstand unexpected attacks of untold dimensions. At the same time, we also have a strong commitment to fundamental innovations that will bring improved, increasingly secure tools to the broad community of network users.

MYTH #3: The objective is a network so secure that it can withstand the evolving and ever more sophisticated assaults.

The need to achieve an impenetrable network belies the fact that even if we succeed in scaring away many of the most opportunistic exploiters by better and broader deployment of enhanced security tools; there is still the likelihood that some attacks will succeed. To this point, we must heed the words of Julia Allen and other colleagues at the Carnegie Mellon's Software Engineering Institute: the point is not to prevent every attack but is to make sure that no attack succeeds in bringing down the institution. The point is not to be blindly secure, but rather to be thoughtfully survivable.

In the final analysis, all of us must strive for a system of operating principles that means that no attack will succeed in disabling the user or its institution.

We must stop believing that firewalls, intrusion detection systems and log monitoring is adequate security. These are only tools of security. A comprehensive approach that entails those tools, as well as network intelligence on impending or imminent attacks is the only viable solution for success. If we consider this a war on cyber attacks, then we must treat it as such. No military commander would suggest that his troops simply wait in foxholes and return fire when fired upon. They would insist on early warning systems and detailed intelligence about their targets and movements. This is the direction we must head in the war on cyber attacks.

In conclusion, the solutions to our cyber security challenge require three commitments.

First, we must provide incentives to all users to make the investments in hygiene practices and tools necessary and appropriate to their status on the Internet.

Second, we must provide incentives to infrastructure custodians, such as VeriSign, to maintain the investments in research and development to provide the innovative tools that meet the ever-evolving threat to our networks from the many sources we have heard about today.

Last, we must provide government at the national and international levels with both forensic tools and investigative training and powers to reach those who are attacking our networks, and through those attacks seek to impact our way of life and our opportunity to contribute to better lives around the world.

VeriSign believes that these actions will improve the overall health and well being of the Internet, but none are magic solutions or silver bullets. True long term health and well being of our information systems will take time and everyone's efforts. Again, this is as much a responsibility of people as it is of technology.

Thank you Mr. Chairman and members of the committee for the opportunity to testify before you today.

Mr. UPTON. Thank you.

Dr. Hancock.

STATEMENT OF WILLIAM HANCOCK

Mr. HANCOCK. Thank you, Mr. Chairman.

My name is Dr. Bill Hancock. I am the Vice President of Security and Chief Security Officer of Cable & Wireless, a large inter-

national telecommunications and hosting company. I am Chairman of the National Reliability and Interoperability Council Focus Group 1B on cybersecurity, a federally authorized council of advisors to the FCC; and I am also the Chairman of the Board of the Internet Security Alliance and appear before you here today on behalf of the nearly 60 members of the Internet Security Alliance.

I am pleased to note that four of the five witnesses that we have before you here today are also members of the Internet Security Alliance, testifying further proof that the Internet Security Alliance has a convicted and overarching concern with security on the Internet and through its member companies.

Among the beliefs of the NIS Alliance is the Internet is primarily owned and operated by private organizations and therefore it is the private sector's responsibility for aggressively securing the Internet environment.

Information security on the Internet is grossly inadequate. This is proven over and over again by different types of attacks and malfeasance that occurs.

A great deal of security requirements—enhancements, excuse me—can occur through application of basic technologies and through advanced education and security awareness.

Technology, while critical to the security industry, will not be enough to provide a safe and secure Internet environment.

To improve overall cybersecurity, creative structures—you have to excuse, Mr. Chairman. I am legally blind, and therefore it takes a minute—

Mr. UPTON. I understand. Don't worry.

Mr. HANCOCK. Government is going to be a critical partner in—ultimately, a partnership between industry and the government is going to need to exist to be able to create a substantial difference and change in the current situation environments and Internet security.

I am what we call in the security business a “gray beard,” which basically means that I have had enough stress and enough age to go along with it dealing with security problems from day to day. When a worm or a virus hits our infrastructure, invariably it is one of my customers that gets hit. My customers will then call us up, and we have to leap into action and go back and deal with the problem at hand.

Sometimes the viruses and worms that we get are rather silly, such as one that was called Giggles some years ago that caused your PC to giggle incessantly. Some of them are very serious that cause the depositing of certain types of technologies onto the PC itself or onto any kind of machine that may be affected, and this includes Unix and Macintosh machines.

Over time, the initial aspects of viruses were actually part of an elaborate game that was played at Bell Labs called CPU Wars. The purpose of CPU Wars was to go back and learn more about operating systems by infecting each others' machines. Over time, this has become a virus writing technique.

Historically, viruses do not leap from machine to machine. Viruses infect and hurt the machine upon which they are on as they become malicious code over the years.

Over time, other methods of moving this type of information around have occurred. In 1988, as a consultant to the National Aeronautics and Space Administration, I sat there with many of my partners totally appalled watching a worm, the first one that we know of, hit the Internet now known as the Morris worm and cause debilitating capabilities—or, excuse me, debilitating all functionality on the network itself.

In those days, the number of people that were on the Internet numbered in the thousands; and getting folks on the phone to find out what was going on was rather trivial. Such is not the case today with over 655 million users of the Internet.

With the conditions for development of viruses and worms remaining as is, I expect the following situations to develop in the very near future:

No. 1, I believe that infection of what we call the invisible networking devices—invisible networking devices are those which historically have not been networked but are networked now. These include things such as DVD players. They include such things as cable boxes. They include automotive electronic systems, radio frequency ID tag systems, even things like parking lot gate attendant systems. All these types of infrastructures now have network connections. All these types of infrastructures now are becoming more and more sophisticated, and all of them eventually will be affected by these type of operations, either by network outages or because of the infections themselves.

Simultaneously, we all invest and use more and more commercial off-the-shelf technologies, and those technologies make for a common platform environment for viruses and worms to spread.

We believe also that worms and viruses will result in hybrid attacks against communications infrastructures due to the lack of security controls and working protocols. Most protocols that are used in the case of Internet and other types of environments were developed in the 1970's, and these are your transport protocols, network routing protocols and so forth. Those protocols have not improved in security controls or capabilities in the last 30 years.

We will also find that other types of building block protocols such as Abstract Syntax Notation .1 will also cause debilitating concern and debilitating results if this is used as part of a virus or a worm environment.

Use of viruses and worms also we believe will be a problem in the near future for the simple fact that we know that nation states and other types of organized intelligence operations are using these types of things as test beds for potential cyberwarfare. The result is that, while there are an awful lot of viruses and worms that do attack the Internet and that do attack individuals and many of these are written by people who have ulterior motives in mind, there are some situations that have been documented that are done by nation states with the ultimate purpose of a precursor either to an attack, a terrorist operation or other types of malicious intent toward the US economy.

While there are plenty of disturbing trends in virus development, we believe there are certain issues that the Internet Security Alliance is definitely concerned about.

No. 1 is companies that provide critical services such as utilities, transport and petrochemical type of activities are connecting more and more of their closed circuit networks and closed circuit environments that have historically been on private networks are now being connected to public networks such as Internet. As a result, a worm or virus infestation will now go back over and infect these types of environments which can cause serious problems throughout the infrastructure.

Home consumer PCs are becoming increasingly targeted by worms and viruses as a way to go back and attack other types of environments, and they become part or chains of attack systems known as Zombies. In these type of environments denial of service attacks and other types of worm attacks can have debilitating results. The cure for such infestations is a long way off, and it is going to require a partnership between the government and industry.

We know that base research in network security improvements, improvement of security technologies, legislative efforts and other types of activities involved with the actual limitation of worms and viruses will have a long-term effect on trying to cure.

One big problem that we keep running into that we are very concerned about is the fact law enforcement is typically hampered due a lack of tools, lack of investment and a lack of skill sets. Last year, for instance, there were very, very few virus writer arrests that were done worldwide. In fact, it numbers less than 10; and, at the same time, well over 100 to 200 viruses a month are generated.

Perhaps the most ironic part of viruses and worm infestation throughout the infrastructure is not the cost to repair or the cost to prevent the infection. It is the cost of entry point. In the case of biological, chemical or nuclear terrorism, the cost is either hundreds of thousands or millions of dollar, having to do with the purchase of the weapons, deployment, training of individuals. In the case of dealing with viruses and worms, the entry point costs to going back and infecting an infrastructure is very simple. It is a PC with an Internet connection.

With that, Mr. Chairman, thank you very much.

[The prepared statement of William Hancock follows:]

PREPARED STATEMENT OF WILLIAM HANCOCK, CHAIRMAN, INTERNET SECURITY ALLIANCE

Thank you Mr. Chairman. My name is Dr. William Hancock. I am Vice President of Security and Chief Security Officer of Cable & Wireless, a large multinational telecommunications and hosting company. I am Chairman of the National Reliability and Interoperability Council (NRIC) Focus Group 1B, Cybersecurity, a federally authorized council of advisors to the FCC. I am also the Chairman of the Board of the Internet Security Alliance. I appear here today on behalf of the nearly 60 member companies of the Internet Security Alliance.

The Internet Security Alliance was created in April of 2001, six months prior to 9/11 as a collaboration of the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University and the Electronic Industries Alliance as well as founding membership of well known international companies with high interest in security issues related to Internet commerce.

I am pleased to note that four of the five witnesses before you this morning are members of the IS Alliance. This doesn't surprise me since members of the Alliance engage in a broad range of activities designed to enhance information security not just for themselves but for all of us who make up the world-wide Internet community.

We are an international, inter-industry group of companies dedicated to expanding cyber security through information sharing, best practices, standards development, education and training, public policy development, international outreach to trusted partners and the creation of market-based incentive programs to improve information security.

Among the core beliefs of the IS Alliance are the following:

1. The Internet is primarily owned and operated by private organizations and therefore it is the private sector's responsibility to aggressively secure the Internet.
2. Information security on the Internet is grossly inadequate.
3. A great deal of security enhancements can occur through application of basic technologies and through enhanced education and security awareness.
4. Technology, while critical to security, will not be enough to provide a safe and secure Internet environment.
5. To improve overall cyber security, creative structures, thought and incentives may need to evolve to provide continued security assurance from the home PC to the large corporate network environments.
6. Government is a critical partner, but, ultimately, the industry must shoulder a substantial responsibility and demonstrate leadership in this field if we are to eventually succeed.

As what we in the security business call a "grey beard," I have been a technical expert, "insider" and leader in the development and deployment of networking and security technologies for over 30 years. While such a span of time might tend to make one wax philosophical about viruses and worms, I tend to have a reality-based perspective as an active practitioner of security on one of the largest network infrastructures in the world. When worms and viruses hit infrastructures, to me it's not a statistic where some other company was taken to the pavement: it's often one of my customers where I and my security teams are expected to leap into action and solve the crisis at hand.

As a security practitioner, I saw the technical games that were the genesis of modern computer viral infections. A computer virus is a man-made code component that attacks computer software and causes a variety of debilitating conditions. Most folks in the security community attribute initial virus development as part of a technical game at Bell Labs in the late 1960's called "CPU Wars," where developers of operating systems would deliberately create infestation code and place it on each other's machines. This action typically resulted in machine disruptions, funny messages on screens and other types of computing interruptions. There were strict rules, however—infestations had to be non-propagative, they could not cause destruction, stop applications from executing and they could not execute during normal hours of operations. Infestations had to be removable on demand. The initial purpose of such games and pranks were to learn, creatively, about how operating systems and computers worked and to share discoveries and ideas in a creative way.

Such is not the case today.

Viruses are a main staple of the hacking community as a method of disrupting programs and systems for a variety of purposes. Some virus-writing efforts are for personal motivations to hurt a specific company, product or service. Some are written by skilled programmers with serious social development or emotional problems as a means of self-expression. Other viruses are written by "gangs" of programmers who have a specific political agenda or by those who have a need to express social will. Still other viruses are written by nation-states as part of their cyberwarfare development efforts to debilitate infrastructure in today's modern technology-dependent warfare environments. There are entities that write viruses under contract to attack competitors and their infrastructure. There are disgruntled employees who seek revenge on their former corporate masters. Viruses are written for a wide variety of reasons but are broadly categorized as being written for social dysfunctional reasons or for the purposes of economic disruption.

Viruses do not self-propagate. They attack whatever system upon which they are activated and perform their damage on that system. Some virus writers have gotten creative with the explosive use of email and have devised ways for viruses to be propagated by email programs and systems. While it appears that a virus "moves," the technical reality is that the virus does not self-propagate—it needs assistance from an external program such as e-mail or from a file transfer action to move from system to system. With the worldwide proliferation of email in the last five years, this makes movement of viruses from one system to another painfully trivial.

Viruses have a variety of effects on businesses. Some are just annoying, such as one of the early viruses called "giggle," which caused a PC to play a giggling voice continually through the PC's speakers for hours upon end. Other viruses destroy software at great corporate cost. One disgruntled employee case I worked on some years ago with the FBI involved an individual who was fired for hacking into the

human resources system and changing his salary. After being fired, he went home, downloaded a piece of malicious code from an Internet underground hacking site and created a small program that would delete all contents of a user's hard drive. He then created a fake email account on a popular public email site and emailed the virus to all the staff at the company with a notation that the file contained a speech from the company's president and that it was being sent so that employees could hear it. Upon "playing" the file, the virus wiped out the hard drive. 1279 employees were sent the virus—710 ran the program and their entire systems had to be rebuilt. The overall cost to correct the damage caused by this one virus at this company was almost one million dollars. You can imagine the horrific cost to repair such damage at a large defense contractor, financial institution or manufacturing concern.

Many more malicious and wide-spread viruses are seen "in the wild" on the Internet on a daily basis. Many are written with Russian, Chinese and other languages in comments in their code. Some have direct ties to organized crime, especially outside the US. Many are propagated from commonly known havens for virus writers where there is no fear of legal prosecution or where the technical skills of the government to prosecute are minimal or non-existent. Some estimates are as many as 100 or more computer viruses or their variants are released world-wide on a monthly basis. The costs to protect against viruses and contain them when they hit can easily be quantified world-wide in the billions of dollars.

In 1988, at the genesis of commercial use of the Internet, I was working at NASA's Langley facility as a consultant when the now-famous Morris worm hit the Internet. We all scratched our heads and initially thought there was a network infrastructure problem. What we did not know was that a young student at Cornell University had created a self-replicating program which would move, very rapidly, from computer to computer, attempting to replicate itself as fast as possible throughout all connected computers. Back then, the Internet was small enough that all the major network control area personnel knew each other personally. We could all get on a conference call and discuss what was going on and coordinate a response. It caused such a serious outage of the Internet that many organizations, to include CERT/CC (represented here today), were founded to serve as an early-warning and solutions service for what was recognized as a new security threat with explosive growth potential. Needless to say, with the estimated 655 million worldwide users of Internet, getting together on a worm attack conference call has become rather problematic.

A worm is typically an autonomous self-propagating program which travels from machine to machine, executing its payload. They do not need the assistance of other standard programs, such as email servers, and can move from system to system using an exploit in a program or protocol. A worm typically consists of a "movement" component, a propagation component and a payload, which may contain nothing at all, self-executing code or a malicious viral infection. Payloads seen in the last couple of years have consisted of a system subversion methodology called a "root kit," where a hacker may later take total control of a system, using standard "known" viruses or defacement tools for automatically defacing websites. For instance, in May 2001, a hacking group that called themselves the Honkers Union of China defaced several hundred thousand websites using a worm that defaced the victim's website with a banner containing the hacker's name. The worm would then rapidly attempt to propagate itself to other sites.

Most worms in today's environment propagate from system to system using known vulnerabilities and attempting to exploit a system based upon those vulnerabilities. In many cases, proper patching against known vulnerabilities or disabling technical components that are not needed for operations would prevent the attack and subsequent propagation of many worms. For instance, on January 25th of this year, a worm called "Slammer" attacked Internet systems via a known vulnerability in a popular database program—one for which the corrective patch had existed for over 7 months. Sites that were patched simply were not affected. Sites that blocked all network entry points for all programs, except those that were open for production programs, with technologies such as firewalls were similarly not affected. Unfortunately, much of the Internet community using the database had not properly applied those patches and they were severely debilitated for almost three days as a result of such negligence.

Some worms have been written to attempt to hurt specific Internet addresses such as whitehouse.gov and software manufacturing companies. Studies of the various types of worms seen in the last two years suggest that some are being used to probe, experiment and test methods in which to infiltrate infrastructures throughout the world. Having reviewed many of them and examined the code personally, it is readily apparent to me that some were written by very professional,

highly trained programmers who could have easily done substantially more damage than they did—if they wanted to. When professionally written worms appear, they gain extra attention from within the security community as it usually is an indication that someone very serious about their efforts is setting something up for later use in a more destructive way.

The use of worm-based techniques of propagation, combined with virus development techniques, is causing new problems for companies and consumers alike. A good example is the recent and continuing propagation of the SoBig worm/virus technology that was and is still used by SPAMmers. SoBig and its variants are commonly used by SPAMmers to distribute a compact email server system to computers which previously did not have such capability. The unwitting victims, such as a broadband cable-connected home PC, are favorite targets of SPAMmers. By doing this, the numbers of email servers capable of sending SPAM to users on any given day has jumped from a couple of hundred thousand or so to several million. This type of technological approach to SPAMming has resulted in an exponential jump in SPAM emails, bandwidth consumption, and overhead (congestion) throughout the Internet.

While most of the uses of viruses and worms are typically malicious or at least inconvenient in today's environment, this will change over time. Worm technologies are currently being viewed as a potential method to distribute critical security patches to systems on networks. Viruses can be used to distribute applications on some modern operating systems. Some countries have introduced legislation to outlaw all use of viruses and worms in all forms. This is a short-sighted and a simplex application of laws to a complex issue as the same technologies are being looked at, very seriously, for use in good—not evil.

With the conditions for development of viruses and worms remaining as-is, I expect the following situations to develop in the near future:

- Infestations of “invisible” infrastructures. Most of us don't think about the software inside a cell phone, automotive electronic system, DVD player, radio frequency ID tag systems, parking lot gate attendant systems, toll booths, wireless luggage bag-to-passenger matching systems, point of sale terminals, automatic door openers, letter sorters, printing presses and many others. As these technologies become more sophisticated, so do their connectivity methods and operating environments. Companies that produce such products migrate towards general-use commercial off-the-shelf (COTS) technologies, which allow greater opportunities for attack.
- Worm, virus and hybrid attacks against communications infrastructures due to lack of security controls in base networking protocols and “building block” protocols such as Abstract Syntax Notation.1 (ASN.1). Much of the communications infrastructure of the world is built on protocol security concepts developed in the 1970's which do not translate well into today's technical security needs.
- Use of viruses and worms by terrorist organizations as a way to deteriorate, disrupt and disable economic and social support systems in use by countries dedicated to anti-terrorist efforts. As horrible and malicious as the various physical attacks have been by terrorists against the United States, those effects are minimal compared to a debilitating attack by a worm against our financial, transport or utility infrastructures.
- Accelerated sponsorship by hostile nation-states where the use of cyber attack is a rapid method of furthering a country's political and economic goals (cyber warfare and information operations methodologies).
- Worms/viruses that “jump” between operating environments and applications. Some have shown this capability already and it's a rapidly growing trend.

While there are many disturbing trends in virus and worm development, there are certain issues which IS Alliance is particularly concerned about:

1. Companies that provide critical services, such as utilities, transport and petrochemical entities are interconnecting historically isolated networks with Internet facilities. This results in such networks being attacked and infested with viruses and worms that cause the networks to become disabled and this can critically affect infrastructure.
2. Home consumer PCs are being increasingly targeted by viruses, worms and hybrids harnessed for use as part of world-wide malicious “chains” of attack systems (known as Zombies) to effect Distributed Denial of Service (DDoS) and worm attacks against Internet connected entities
3. Research and development into new security encodings and methods in base network protocols needs to be accelerated to help offset the continued development of malicious code used to attack infrastructure

4. Lack of law enforcement actions, globally, in the prosecution and arrest of virus and worm developers. An extremely low number of persons involved in the development and distribution of malicious code are ever identified or prosecuted due to a lack of technical tools, skills and personnel in most law enforcement organizations.
5. Inclusion of basic system and application protection methodologies by developers of same. Basic technologies such as polymorphic checksums and cryptographic signature methods are well known and available. Such technologies could be used by all manner of developers to stop infestations and propagation of these malicious code segments.
6. Lack of senior corporate management to act properly, responsibly, rationally and quickly in the deployment of security technologies to prevent infestations and propagation of malicious code. Too many companies still do not invest in the basics.
7. Acknowledgement that viruses and worms are truly a multinational problem. While leadership by technologically advanced countries is crucial, introduction of viruses and worms into network infrastructure is easily done by the "weakest link" in connectivity—a small country with no laws on cybercrime, no assets to protect, and no national will or means to prosecute perpetrators becomes the entry point for the world to be attacked. Remember that access to a small country's infrastructure does not require a physical presence—even a dial-up connection from anywhere on the planet will do just fine.

The "cure" for infestations is a long way off and will require partnership with industry and government to solve. Base research in network security improvements, deployment of security technologies, legislative efforts to prevent criminal use of worms and viruses, improvement in operating systems to stop infestations, application-level security technologies, law enforcement prosecution of cyber criminals involved in the creation and distribution of virus and worm technologies, improvement in base critical infrastructure and education and training through all levels of corporations, government and society will need to be combined to come up with effective eradication solutions.

Perhaps the most ironic aspect of viruses and worms is not just the cost to repair or prevent infestation—it's not like biological, chemical or nuclear terrorism where thousands or millions of dollars are required to make such an attack happen. It's just the entry cost necessary to create and distribute worms and viruses: A PC with an Internet connection.

With this, Mr. Chairman, ladies and gentlemen, I conclude my opening remarks. Thank you for your efforts and your leadership in this important topic.

Mr. UPTON. Thank you very much.

Mr. Wong.

STATEMENT OF ARTHUR WONG

Mr. WONG. Chairman Upton, members of the subcommittee, thank you for the opportunity to provide testimony on this important topic.

My name is Arthur Wong, and I am the Vice President of Response for Symantec, the world leader in Internet security technology, providing a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers.

We are at an important juncture regarding cybersecurity. The threats we are seeing today are more sophisticated, more aggressive and are able to spread more rapidly than ever before. Equally important, the time it takes from the discovery of a new vulnerability to the time the vulnerability is exploited by the launch of a worm or a blended threat is rapidly shrinking. These two phenomena have made the Internet increasingly vulnerable to attack.

For example, the Slammer worm attack from January of this year exploited a vulnerability discovered 6 months earlier. In August this year, the time window changed significantly with the re-

lease of the Blaster worm. Blaster was launched just 26 days after the discovery of the vulnerability it exploited.

We are already beginning to see even the early stages of what we call flash threats. These threats are near instant in their delivery and where human reaction time is probably not fast enough to prevent attacks that occur globally in minutes or mere seconds. The Slammer worm in January spread globally within 15 minutes.

Let me give you some additional insight based on our recently released Internet Security Threat Report, a comprehensive semi-annual view of cybersecurity activity. The report documented over 1,400 new vulnerabilities, a 12 percent increase from last year. Sixty-six percent of all the new attacks this year documented were based upon highly severe vulnerabilities.

Now, early warning and alerting capabilities, strong patch management and solid internal processes to respond to potential threat may be the difference between protecting critical systems and having them actually compromised.

Let me now turn to two key areas, corporate security governance and user awareness.

Corporate IT security cannot be an afterthought or an add-on approach. It should be integrated into the overall management plan for an organization. In today's connected world, we rely heavily on our IT infrastructure to conduct business and should not be compromised due to lack of security measures.

In developing a cybersecurity plan, we believe there should be a focus on the following areas: business continuity, regulatory compliance, enabling "e" initiatives and the establishment of a security policy and implementation plan. All of this must be done balancing risk and managing costs to ensure system availability and security.

IT security requires a new level of governance at the most senior levels. It requires a top-down approach that reaches across an organization's departments and functions. It requires the creation of a culture of security.

Let me now turn to education and awareness. A vulnerable system, regardless of whether it is a home user surfing the Web on a broadband connection, a wireless mobile computer at Starbucks, or a telecommuter working from home, all can open the door to a virus or worm attack.

I would point out that we wrongly think of the individual user as merely a home user. Users are also employees, customers, business partners of enterprises and companies.

We also need to educate employees through a well-organized security training program. Symantec has taken an active role in promoting a broad-based awareness campaign through our participation as a founding member of the National Cyber Security Alliance.

In partnership with the Department of Homeland Security and the Ad Council, the Alliance recently announced a \$1.8 million national cybersecurity awareness campaign of which we are a major contributor and supporter of. The program will be designed to educate the home and small business users on the importance of using anti-virus and firewall technology, as well as tips to defend against on-line fraud.

A recent study by the National Cyber Security Alliance showed about 67 percent of high-speed Internet users do not use firewalls,

and more than 60 percent do not regularly update their anti-virus software, confirming the need for this broad-based campaign.

Symantec has created a free tool on our Web site called Symantec Security Check that scans an individual system for vulnerabilities and viruses. We have conducted over 50 million scans in 2 years. Now, of the 3.9 million people who were scanned and agreed to submit their data to us, 24 percent did not have any virus protection whatsoever; and 9 percent of those that did have some type of anti-virus solution did not regularly update it. In addition, of the 1.35 million users who submitted their data to our virus detection scan, 35 percent were already infected with a virus or worm.

The work by the National Cyber Security Alliance is a great example of the type of public-private partnership essential to promoting a safe and secure computing environment. Security is more than just installing a piece of software. It is the use of best practices, updating your anti-virus and practicing secure computing to ensure that systems are safe and the Nation's infrastructure is more secure.

Thank you.

[The prepared statement of Arthur Wong follows:]

PREPARED STATEMENT OF ARTHUR WONG, VICE PRESIDENT, RESPONSE, SYMANTEC CORPORATION

Chairman Upton, Ranking Member Markey, members of the Subcommittee, thank you for the opportunity to provide testimony today on computer Viruses. This is a timely and important topic and on behalf of Symantec, I appreciate your willingness to examine the issue and challenges surrounding it.

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of client, gateway and server security solutions for virus protection, firewalls and virtual private networks, vulnerability management, intrusion detection, Internet content and e-mail filtering, remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries.

We are at an important juncture with regard to cyber security. The threats we are seeing today are more sophisticated, more aggressive and are able to spread more rapidly than ever before. Equally important, the time from the discovery of a new vulnerability to the release of an exploit targeting that vulnerability is rapidly shrinking. I make the analogy of an exploit being an "unlocked door" of a building and an exploit being a break-in by someone who knows about the unlocked door. These two phenomena have made the Internet increasingly vulnerable to attack.

We are already beginning to see the early stages of what are called flash threats, threats that are near instant in their delivery. These are threats in which human reaction time is probably not fast enough. A good example would be the recent Slammer worm, which, at it's a peak rate, infected 90 percent of the vulnerable systems in just 15 minutes. This speed of propagation, combined with the reduction of the time to exploitation, raises serious issues about the approach our nation is taking to protect our networks.

We have taken the initial steps to improve our cyber security, from the largest corporations or infrastructures to the individual end user, but security is an evolving process and we must continue to be aggressive in our corporate IT security governance and in educating the individual user about good cyber security practices.

Congress passed the Federal Information Security Management Act (FISMA) to improve the protection of government systems. This risk-based management approach provides a guideline for Agencies to improve the protection of their critical assets.

In the private sector, associations like the Business Software Alliance and TechNet are working on information security governance projects to assist the pri-

vate sector on improving the protection of their infrastructure. I am pleased that Symantec is a part of both of those projects.

I would also point to the upcoming Department of Homeland Security Summit scheduled for December. The summit's intent is to bring together government and industry leaders to work on implementing the National Strategy to Secure Cyberspace. This is a positive sign of the commitment to work together on this important issue.

But more needs to be done. If anything, the recent attacks during the month of August served as a "wake-up" to all of us. In fact, the threat of major cyber attacks causing significant damage to our infrastructure is real and still exists today.

Let me give some additional insight into the nature of the threats we are seeing with information from our recently released Internet Security Threat Report, a comprehensive semi-annual view of cyber security activity. The report covers information on vulnerability discoveries, malicious code trends and network-based attacks. I have included a copy of the report for submission with this testimony.

The report represents the distillation of data from over 500 Symantec managed security customers and over 20,000 registered sensors monitoring worldwide network activity in more than 180 countries. We would argue that it provides the most complete view of the health of the Internet available anywhere today.

As I mentioned earlier, the time from vulnerability discovery to exploit is rapidly shrinking. For example, the SQL Slammer worm attack from January of this year, exploited a vulnerability discovered about six months earlier. Just a few months later that benchmark changed significantly with the release of the Blaster worm. This blended threat exploited a vulnerability just 26 days after disclosure.

We have also seen that 64 percent of all new attacks targeted vulnerabilities less than one year old. Moreover, of all the new attacks documented in the first half of this year, 66 percent targeted what would be classified as highly severe vulnerabilities. Symantec documented over 1400 new vulnerabilities, a 12 percent increase from last year. In looking at the severity of these new vulnerabilities, we saw a 6 percent increase in those carrying a "high" severity rating and a 21 percent increase in those of "moderate" severity. These trends should be a major concern to all of us. As they continue, we will need new security paradigms to appropriately protect our cyber-infrastructure.

Early warning and alerting capabilities, strong patch management, and solid internal processes to respond when a new vulnerability is discovered, may be the difference between protecting critical systems and having them compromised.

With regard to malicious code trends, we observed a much more aggressive attack pattern. The Blaster worm, as an example, infected systems at an average rate of 2,500 computers per hour.

We are also starting to see the use of viruses and worms to attack newer applications, such as instant messaging and peer to peer networking.

In fact, of the top 50 malicious code submissions we received in our laboratory during the first half of this year, 19 used peer-to-peer and/or instant messaging applications—an increase of almost 400 percent in just one year.

So, the trends suggest that the overall rate of attack activity rose 19 percent. Companies experienced, on average, 38 attacks per week compared to 32 for same period last year.

By highlighting some of these key findings, we see the importance of prioritizing cyber security at work and at home.

I would like to focus on two key areas I believe are important to improving cyber security of our IT infrastructure: Corporate IT security governance and user awareness.

Corporate IT security cannot continue to be an afterthought or add-on approach. It should be integrated into the overall management plan for an organization. In today's connected world, we rely heavily on our IT infrastructure to conduct business, and it should not be compromised due to a lack of security measures.

The resource constraints that many organizations are facing, coupled with the increasing rate of attacks, make this a daunting challenge. In many instances, these attacks are dealt with in a reactive rather than a proactive manner, making the task even more difficult.

In developing a cyber security plan, we believe it should focus on the following areas: ensuring overall business continuity, adhering to regulatory compliance, enabling organizations for their "e" initiatives, and, establishment of a security policy and implementation plan. All of this must be done with a watchful eye on balancing risk and managing cost to ensure both system availability and security.

In discussions with enterprise organizations, they cite three main drivers of the need to look at security in a more holistic manner. They include the disappearing perimeter, the increase in threats and the lack of security expertise.

The question really is “how do we adequately address these issues?” I believe IT security requires a new level of governance at the senior level. It requires a top down approach that reaches across the organization’s departments and functions. It requires the creation of a culture of security.

IT governance must be a part of the overall governance of an organization. Doing so will ensure that IT is aligned with the organization to deliver value to its constituents, that IT resources are responsibly utilized and that IT risks are mitigated and managed appropriately. Taking this a step further, information security should also fit in this broader view. For example, information security reports should go to senior executives in an organization and information security audits should be part of the overall audit program.

Furthermore, implementing security with real-time risk management is a key to preparation and protection. Organizations need to know where they are vulnerable, establish benchmark security levels and policies that will ensure compliance.

Let me now turn to education and awareness. We have often heard the statement that we, as individual users of the Internet, have an obligation to protect our piece of cyber space.” I firmly believe this is true.

A vulnerable system, regardless of whether it is a home user surfing the web on a broadband connection, a wireless mobile computer at Starbucks, or a telecommuter working from home, all can open the door to threats.

As we continue to see increased computing power for the individual user and continued adoption of high-speed connections, we must focus on providing a safe and secure environment for that user, which includes using a firewall and a regularly updated anti-virus program.

I would point out that we often think of the individual user as only the home user, a view that is short sighted. As mobile computing becomes more pervasive we need to be aware at the enterprise of the potential holes to the network that could open up from customers, business partners or employees.

The perimeter to the enterprise is disappearing and steps must be taken to protect those critical assets not just at the gateway, but at all the end-points or access points being used in today’s environment.

This means more than just implementing technology solutions. It means educating the employees through a well-organized security-training program. Employees need to be armed with the knowledge to responsibly protect our networks.

Symantec has taken an active role in promoting a broad-based awareness campaign through our participation as a founding member of the National Cyber Security Alliance.

In partnership with the Department of Homeland Security and the Ad Council, the Alliance recently announced a \$1.8 million national cybersecurity awareness campaign. Symantec is a major supporter of this effort along with other leaders from industry and government.

The Alliance program will be designed to educate the home and small business users on the importance of using anti-virus and firewall technology, as well as tips to defend against online fraud. Further information from the Alliance can be found at www.staysafeonline.info.

A recent study by the National Cyber Security Alliance confirms the need for this broad-based campaign. That study showed that about 67 percent of high speed Internet users do not use firewalls and more than 60 percent do not regularly update their anti-virus software.

In addition to the National Cyber Security Alliance, Symantec has also created a tool that home users and small businesses can use. This tool, called Symantec Security Check, can be found at <http://www.symantec.com/securitycheck> , It is free service that scans an individual’s system for vulnerabilities. To date we have conducted over 50 million scans. Of the 3.9 million people who were scanned and agreed to submit their data, 24 percent did not have any anti-virus protection, and 9 percent of those that did have some type of anti-virus solution did not regularly update their definitions. In addition, of the 1.35 million users who agreed to submit their data to our virus detection scan, 35 percent were infected with viruses or worms.

We need to broadly get the message out about the dangers and threats to our Internet infrastructure. The work by the National Cyber Security Alliance is a great example of the type of public-private partnership that is essential to promoting a safe and secure computing environment, and ultimately better protecting our critical infrastructure.

Let me close by saying that education and awareness of the individual whether in the largest multi-national corporation, small business or the home user is critical. Security is more than just installing a piece of software, it is using best practices,

updating your anti-virus and practicing safe and secure computing to ensure that systems are safe and the nation's infrastructure is more secure.

Thank you.

Mr. UPTON. Thank you very much.

Mr. Holleyman.

STATEMENT OF ROBERT W. HOLLEYMAN, II

Mr. HOLLEYMAN. Chairman Upton and members of the subcommittee, I appreciate the opportunity to testify today on behalf of the member companies of the Business Software Alliance. Our companies are the leading developers of personal computer software, enterprise software, as well as are leading hardware partners and e-commerce providers.

I would like to address three points in my testimony today that I think are important as we look to this framework for protecting ourselves against viruses and worms not only here in the U.S. But internationally.

First, we need to create an environment in which information security is a priority for every company, every government, every household and every developer; second, we need to enhance law enforcement's capabilities to treat destructive viruses as the serious crimes that they are; and, third, we need to build on our international cooperation using U.S. Leadership with key partners to recognize that viruses are, more often than not, international in scope.

I believe the scope of the problem has been well articulated by witnesses on this panel before me, so I will not go back through that scope except to say that the number of attacks are growing and this is a growing problem.

At the BSA, in our years working on the issue of cybersecurity, we focused on both industry-led best practices and legislative reforms. In the software industry, we have redoubled our efforts to build more reliable, better and more secure products. Security is the top priority for each and every CEO in the companies that we represent, and we believe that we have a responsibility and are stepping up to the plate to ensure that that culture of security is within all of our companies.

We also believe that the culture of security needs to be extended as a senior management priority for every company. BSA has created a CEO-level task force on this issue. We want to ensure that private-sector participation is a key part of creating this culture of security, because indeed the private sector owns, operates and maintains nearly 90 percent of the information networks.

BSA has a just-released Framework for Action that outlines specific roles for business unit heads, senior managers, CIOs and CEOs themselves. As part of that, we analyze the field. There is a lot of great information that has been developed by governments, by private-sector groups about what needs to be done. Much of that information, however, is very technical in nature, and part of what we need in closing these gaps is to create a framework so that not only the technologists can understand this but senior managers can understand this, and we also need to take this to the home and users of small businesses as well.

As part of this, BSA has released a checklist that identifies the type of steps that need to be taken to improving cybersecurity for individuals, for small organizations, for medium- to large-sized enterprises and for government agencies. It recognizes, appropriately, that everyone has a role in this, but there are also levels of technical understanding that vary, and we would be happy to work with this subcommittee in making sure that those sorts of checklists are disseminated.

We also are working in the area of law enforcement. Law enforcement must have tools that are at least equal to those of the cybercriminals that they are trying to combat. Many times cybercrime is not yet perceived as a real crime. There is insufficient deterrence for cybercriminals and potential terrorists.

To deal with this, we have to raise awareness globally that computer attacks are serious. We need to ensure that law enforcement has the right tools. They need the right personnel, they need the right training, they need the right equipment. And, third, we have to deal with the cross-jurisdictional aspects of this, recognizing that many times these crimes need to be pursued across international borders.

Congress has led the way through its efforts in the U.S. Such as the Cybersecurity Enhancement Act approved by Congress last year that increased penalties for people who commit cyberattacks. We need to ensure that those models are replicated around the world.

Finally, this brings me to my last point, which is international cooperation. This is absolutely vital, and I believe this is a unique time for leadership by the U.S. Government in this area. Everyone working in this field, whether they are in industry or law enforcement or political leaders, recognize that we have only begun to scratch the surface in dealing with this problem. There are, however, only a handful of other governments around the world who have begun to focus the same level of attention that we have.

The U.S. just reached an agreement with Japan, a memorandum of understanding on fighting cybercrime and cyberterrorism. The European Union is creating a network and information security agency. There is a great opportunity in working with Australia, another leader, and Canada, another leader, to create this international framework that allows us to deal with this as a matter of policy, a matter of law enforcement and a matter of awareness.

As part of this, we want to ensure that the U.S. principles that ensure that there is private-sector leadership, that we develop flexible standards, that will allow new products to be innovative and to come on the marketplace can be deployed. We believe that through these partnerships of technology and throughout the private-sector leadership and the U.S. global effort we can make progress. At BSA, we are committed to working with government as part of this. We welcome the opportunity to testify today to be part of this dialog.

The goal of today's hearing is to look at viruses and worms. The longer term goal is to look at what it takes to create a culture of security, to create more confidence in networks and information networks and to promote economic prosperity.

Thank you.

[The prepared statement of Robert W. Holleyman, II follows:]

PREPARED STATEMENT OF ROBERT HOLLEYMAN, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE (BSA)

Good morning. Chairman Upton, Congressman Markey, Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject: computer viruses. My name is Robert Holleyman and I am President and CEO of the Business Software Alliance (BSA).

BSA represents the world's leading developers of software, hardware and Internet technologies. We are headquartered in Washington, D.C. We also have offices in Europe and Asia and are active in more than 65 countries.

Today I'd like to focus my remarks on laying out a prescription for prevention of cyber attacks and the three critical areas where technology companies and governments need to make progress in order to make our information networks safer:

- First, elevating information security as management priority for every company.
- Second, enhancing law enforcement's capabilities to treat destructive virus attacks as serious crimes, and
- Third, increasing international cooperation to better recognize that viruses are, more often than not, international in scope.

But before I talk about some of these crucial steps that the high-tech industry and governments around the world need to take to mitigate our risks, let me begin by giving you a prognosis for the disease.

- According to preliminary data from a BSA survey of more than 12,000 information security professionals, 65 percent of security professionals believe it is likely that their organization will be hit with a major cyber attack in the next 12 months.

- According to research by Symantec, an estimated 200-300 new viruses are discovered each month, bringing the total number of catalogued viruses and worms to over 65,000.

- Gartner has predicted that cyber crime will double or triple between 2001 and the end of this year. It also believes that by 2005, 60 percent of the security breaches will be financially or politically motivated.

- The cost of viruses to American business is staggering. Business Week and Gartner report that viruses have already cost US businesses \$13 billion this year alone.

As the National Strategy to Secure Cyber Space has clearly articulated, the threats are real, and the solutions are not simple.

At the Business Software Alliance, we have focused much of the last several years on working with businesses and governments to assist them in preparing against potential cyber attacks, and to institute—through both industry-led best practices and legislative reforms—sound policies to help eliminate some of this confusion and maximize our collective cyber preparedness.

Our efforts have encompassed a wide array of topics—from encouraging industry leadership in best information security practices, to opposing technology-specific government standards that would stymie the dynamic evolution of security and anti-virus tools.

Indeed, the software industry has redoubled its own efforts to build better, more reliable, and more secure products. I can tell you with complete certainty that security is the top priority for each and every CEO in our industry. Clearly, our industry has a critical responsibility to make the most secure products possible, and we are stepping up to the plate.

At the same time, there are three areas where we, as a nation, must collectively turn our focus.

INFORMATION SECURITY MANAGEMENT

First, it is imperative that cyber security become a senior management priority for every company. We need to fundamentally recognize that information security is not solely a technical issue, but a corporate management challenge that must be treated as such to make progress. That's why the BSA has created a CEO Task Force on this issue, which is working to elevate cyber security to the level of senior management. We must remember, after all, that the private sector owns nearly 90 percent of the nation's information networks.

We are doing more than just preaching this message, however. The BSA task force recently released a preliminary Framework for Action that outlines specific roles for business unit heads, senior managers, CIOs, and the CEOs themselves. This whitepaper distilled the lessons contained in other policy reports, legislation, and guidelines and found broad consensus on what needs to be done.

The more we do together to promote awareness of information security among corporate executives and accelerate adoption of effective security strategies, the more secure our nation will be.

EFFECTIVE LAW ENFORCEMENT ACTIONS

The second area that needs immediate attention is law enforcement in cyber space. Determined, innovative hackers, virus writers and cyber criminals are constantly working to develop new ways to break into systems—just as criminals in the real world are continually inventing new types of fraud and finding new ways to break into cars or homes. But many cyber crimes are not yet perceived as real crimes. As a result, there is insufficient deterrence for these cyber criminals and potential cyber terrorists.

Let me highlight three areas for further progress:

- *First*, we need to raise awareness globally that computer viruses, worms and denial of service attacks are not clever acts of mischief, but serious crimes that can cause major economic damage, or worse. Just as in the offline world, when criminals steal or attack online, authorities need to be able to find and punish them.
- *Second*, we need to ensure that law enforcement has the resources it needs—personnel, training, and equipment—so that cyber space doesn't turn into a safe haven for hackers, virus writers and other criminals. Governments need access to the same cutting-edge technologies that cyber criminals use, and the ability to coordinate, investigate and enforce.
- *Third*, we need to ensure greater cross-jurisdictional cooperation in investigating cyber attacks. Cyber security is inherently an international issue that requires international solutions. Many of the most recent cyber attacks were international in scope. Continued collaboration, information sharing, and tough laws in every country criminalizing cyber attacks are vital to ensuring that law enforcement can help prevent crime and investigate cyber criminals wherever they may hide.

That brings me to my third and final point:

INTERNATIONAL COOPERATION.

Our cooperative efforts need to extend far beyond law enforcement. Indeed, strong relationships are necessary with Europe and the still small number of countries around the globe that are taking a lead on these issues.

I was in Brussels in June for a major forum that BSA co-organized with leading members of the European Parliament to discuss cyber security, and, specifically, the European Commission's proposed Network and Information Security Agency. It is crucial that the technology industry—and the U.S. government—work closely with the EU to ensure that the structure of this new agency—and any others that are ultimately created around the world—is flexible enough to provide rapid responses to ever-changing security threats. It also needs to be technology-neutral—relying on performance guidelines and best practices rather than technology-limiting standards.

The U.S. has a unique opportunity to build new global partnerships and set baseline standards that reinforce the importance of technology neutrality and private sector leadership.

In closing, let me affirm BSA's belief that successful, constructive partnership by both government and industry is necessary to effectively meet the global information security challenge.

While today's hearing is about making progress in defending against computer viruses and worms, it is really about how we can build faith in our information networks to make them more valuable and effective. To do this, we need a shared commitment to reducing risks and increasing cooperation between businesses, network operators, law enforcement agencies and governments as a whole. The BSA stands committed to playing our part in helping ensure that the nation has a prescription, not just for immunizing ourselves against viruses and worms, but for enabling a safe and healthy digital world that fosters innovation, unleashes human potential, and spurs economic growth.

Thank you and I look forward to your questions.

Mr. UPTON. I want to thank all of you for your fine testimony this morning.

I just—you know, as we woke up to the news this morning, some of us saw it last night, about Microsoft's \$5 million reward mecha-

nism, I think we all applauded that. But, at the same time, we said, is this enough?

When you talk about the number of culprits that were caught this last year, I think—Dr. Hancock, I think it was you that said less than 10, and they have all been pretty high-profile cases. The young man allegedly from Minneapolis, I think it was, a few others that we can remember.

But when you think about the cost to the consumers and businesses as well as individuals, as we look at our own systems at night when we go home, with the anti-virus software packages that we all have, I would guess that it is probably almost every week that I see something pop up on my PC with some report or some request that is made of me to shut things down and restart that software. But with these number of attacks growing, is this a losing battle that we can't catch up?

Mr. HANCOCK. Sir, I believe that it is not a losing battle, but it is a very, very serious one. I think that the thing that you need to understand is that even the people that are caught and the people that have been caught in the last 12 months in many cases were not the original writers of the virus or the worm in question. In many cases, they took the original and mutated it into something else that they themselves produced. This means that we are still having a great deal of trouble trying to find the original writers of many of these types of technologies that we see. We will continue to have that problem as long as there are safe havens around the world and there are places where prosecution does not happen. If there is no repercussion for going back and creating a malevolent environment, then there is no reason for someone to stop.

The other problem that we run into is that in some cases there is serious motive involved with some of these reasons and efforts that people do these things. So one area to look at is to also go back and see how do you dry up the revenue source, and if you can dry up the revenue source a lot of this nonsense will stop.

That is especially the case with spam. All spam involves some sort of revenue source, someone paying to have spam put out there or some sort of way to generate revenue. Most spam messages involve things like, you know, drug refills or potentially other ways to purchase illicit drugs. In those types of situations, there is a profit motive involved; and if you can dry up their profit motive you dry up the spam accordingly. So spam may use worm and virus techniques to get around, but it would stop a lot of it if there were ways to go back and dry up the ways that these people generate revenue for themselves.

Mr. UPTON. What is your—anyone else want to comment on that? Mr. Silva.

Mr. SILVA. Yeah. I would like to comment on the first part of that with respect to Microsoft's issuing a reward for this. I think it is a very commendable thing that they have done. But I think it is also a sign of the times, okay? I mean, this is really at a stage pretty much—it is real money. It is real money, but, you know, the tactics we are having to take now are similar to those of the old West, okay? We are having to offer rewards and bounties for, you know, the villains out there that are attacking our networks.

I agree that we have to do that at this point in time, but it is a scary situation that we are in, that these are the tactics we have to resort to.

Mr. UPTON. What is your guess as to how many of these actually come from overseas? 50 percent? 25 percent? 80 percent?

Mr. PETHIA. I don't certainly have a good guess at that. We have certainly seen historically at different points in time there would be an outburst of viruses coming from some particular part of the world. But I think if you look across time I don't know that there is any single source that stands out above any others.

Mr. HANCOCK. I will comment, Mr. Chairman, that it is my personal experience with several of them recently that some of the more, shall we say, professionally written products that have come out and hit people in viruses and worms have had comments in foreign languages in them, specifically Russian and Chinese. In both of those situations, at least the Russian one, we were able to back-track through our cyberattack tiger team that the worm itself originated from a machine in Australia which we were able to forensically examine. We found out that that machine had been broken into from a location in Russia. Upon further investigation with the Russian computer police in Moscow, it turned out that it was an organized crime operation in progress, where it just basically deposited it to work on the outside. But it was written, according to them, by a potentially organized crime unit in the Russian area.

So we are starting to see a lot of those are being professionally written by people with skill. If you read the comments and you look at the code, they are written by people who know what they are doing and in some cases are actually written in terms of organized crime definitely outside the United States in many cases. But we have seen quite a few of them coming from the Chinese area and also coming from Russia.

Mr. WONG. Chairman Upton, what we have seen—because we monitor over 20,000 devices worldwide in over 182 different countries in the overall scheme of attacks, we have seen that most of these actually originate in the United States attacking people, organizations and infrastructure in the United States. So whether these individual virus writers or these individual viruses or attacks have started somewhere else or not, the main thing that we see overall as a trend is that most of them start here. Most of them are targeted here.

Mr. UPTON. Thank you.

Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

Dr. Hancock, can you give us a little more detail on how spammers are currently using the Sobig worm months after it did such terrible damage to networks nationwide?

Mr. HANCOCK. In terms of what, sir?

Mr. GREEN. Well, in terms of how they continue to use—are they using or continuing to use the worm even after it was discovered?

Mr. HANCOCK. Yes, sir, they are. In fact, I think the current variant is up to level G right now.

I have, through my good friend, Commissioner Orson Swindle at the FTC, he asked me to prepare a talk last May on the future of

spam. I have the dubious honor of now being labeled the “prophet of doom” by the FTC because I got up and said, here is how it is going to happen next and what is going to happen; and I predicted what Sobig turned out to be a full 4 months before it hit the Internet.

The bottom line of this is that what people are doing is that spam is a function of e-mail. To send an e-mail at any given time in the world, you have to have an open relay within an e-mail server. It has been estimated that at any given time there is about 100 to 150,000 of those that are open worldwide. The concept of Sobig is that you not use an existing open relay. Instead, you send software to a particular machine which then deposits an e-mail transmittal system onto a machine that did not have e-mail transmittal capabilities whatsoever, like your home PC.

So what Sobig does that makes it very nasty is that, as it goes around, it infects different machines in a worm-like way. It then downloads a full e-mail service capability to that machine that could not previously generate e-mails. In other words, it becomes an e-mail server. The result is that Sobig and its variants have now come up to an estimated over 1 million active open relays available at any given time, which means that spammers can use those on machines that they could previously not access because they were only limited to whatever open relays are out there.

So the technology of Sobig basically provides—and there are other ones, too, besides Sobig—provides the ability for spammers to use worm technology and worm concepts to deposit malicious code on machines and turn those into spam relay systems. So Sobig does continue to be generated, the new versions. Those new versions find new ways to weasel themselves into different machines and deposit these kinds of spam relay software technology out there to increase the opportunity for spammers to send spam.

Mr. GREEN. Do you think that any of the anti-spam legislation that regulates the unsolicited e-mail with effective law enforcement, the FTC, will help protect businesses from the fusion of the spam and the virus problem?

Mr. HANCOCK. Sir, I am on record with the FTC as saying that I think it will have minimal effect, because the spammers will simply move offshore. There is no legislation in other countries.

Mr. GREEN. Do you think, though, if we actually do something in the United States, as I think one of the witnesses mentioned earlier, then we have to deal with our other countries, our trading partners similar to what you dealt with the Russian computer police, for example?

Mr. HANCOCK. Yes, sir. I think that that is a very good thing to do. But I will caution also, one of the areas that has historically been known for having a lot of problems with computer security is in Romania. I happen to know that—I have actually met with their one computer crime guy in all of Romania, and this poor individual is grossly overwhelmed. And when you start dealing with that kind of situation, I think that there is very good intent by other countries and our trading partners, but there is no investment in their own law enforcement, nor is there any investment in their own infrastructure to go back and prevent these kinds of things from happening. When you have one law enforcement guy in an entire coun-

try dealing with some of the worst problems that come out throughout the entire network infrastructure, it makes a losing proposition even if you go back and try to muscle that particular trade partner.

So I am not defending them and I am not saying it is the right thing to do, but it is a reality.

Mr. GREEN. And, again, everything starts with one step, I guess. So, you know, if you have a strong Federal law like we have some strong State laws, then we can deal with our trading partners. Again, Romania is a country that obviously wants to join the EU, and will have to comply with the same agreements that other countries do with the EU, along with trade with our own country. So at least we have that leverage.

Mr. HANCOCK. No argument, sir. And I am not saying that we should not pass legislation in the United States or that we should not try to contain the problem here. I am simply stating the fact that what will happen and has happened with other types of situations where laws have been passed in a specific country is that the people that exercised the malfeasance just simply moved to another country.

Mr. GREEN. But we shouldn't throw up our hands and surrender?

Mr. HANCOCK. No, absolutely not.

Mr. GREEN. Okay. Thank you.

Mr. UPTON. Mr. Deal.

Mr. DEAL. Thank you, Mr. Chairman.

I want to try to get a handle on this in terms of why this is happening. For a long time I think many of us regarded this as some form of juvenile delinquency for computer geeks; that it was a form of graffiti that was just an act of vandalism. Obviously, with the magnitude of the impact that you have talked about, that even though that is a portion, I am sure, of it, I would like to know what you think the motivations for this problem really are.

Dr. Hancock, you alluded to the issue of profit, profit for spammers, using this as a technique to bypass and get their information out. What other motives are there other than spammer profit? What are the motivations for this? There have been some allusion referenced perhaps to potential terrorism. I don't know that we have had specific examples of that being a motivation. But would the panel care to elaborate on what these motivations are? Something that is this big of a problem, there has got to be something other than just pure fun to see what kind of trouble you can cause in the universe. What are the motives?

Mr. HANCOCK. If you would like to, sir, I can give a first stab and then invite the other panelists, because I am sure they have their opinions as well.

It has been my experience—and I have been involved in over 600 hacker prosecutions—that a vast majority of them are dysfunctional individuals. These are people who literally we bust them at 3 o'clock in the morning, because that is the best time to get them because they are the only ones awake in the house. These are people that have very serious social problems. They do not associate with other folks. It is a way of expressing themselves, using their intellect and using their capabilities. And that tends to be a very large percentage of what we run into.

Another one is, you run into hacker gangs. There are folks out there that—such as Cult of the Dead Cow, Hacking for Gurlz, spelled G-U-R-L-Z, and these types of individuals that believe certain manifestos, and therefore they use these types of techniques to go back and further their manifestos.

Hacking for Gurlz, for instance, has a manifesto that states that information has a soul and yearns to be free, and therefore what they do is they go back and attack in groups people and capabilities and corporate structures to turn information free, because they believe that your Microsoft Word file has a soul and needs to get out. And so there is that sort of mentality out there, and it really does exist and these people really believe these kinds of things.

You have also got the other extremes that basically say that there is evidence that goes worldwide where virus attacks, worm attacks, spam attacks may be against competitors as part of a competitive function. And there are places on the Internet where you can go hire people that will go back and write things and produce spam and produce viruses and worms to go back and attack competitors or attack a competitive infrastructure. And that has been documented in other countries, and it has happened.

There are other things that happen where you are dealing with kids that are just out there messing around. For instance, we have been documenting a lot of what we call script kiddie attacks. The bulk of them happen between 4 o'clock p.m. Pacific time on Friday and 9 o'clock p.m. Pacific time on Sunday, because every kid without a date starts picking on our network. So I am going to start a site called geekdate.com and try to get them some dates and leave us alone. But that is a different problem.

But you will see this whole rash of things that are out there. And then about 5 percent of what we hear that goes on—and I have some anecdotal evidence and also some direct evidence to this effect, nation states that are competitive to the United States or that do not feel politically aligned to the United States. And a good example of that is in May 2001, something called the Honkers Union of China launched a worm attack that basically disabled well over 300,000 Web sites with the defacement of Honkers Union of China banner across all of those. As part of a sympathetic attack, while the attack was in progress, Brazilian hacking teams got involved and started helping propagate the same worm and virus around, simply because the folks down there really don't think very highly of the United States in many cases. And Brazil is becoming a very large place where you can get a lot of hacks, you can hire people, you can get these kinds of things out there.

So there is an enormous range of reasons why people do these types of things. Some of them are profit-oriented, some of them are socially dysfunctional.

Mr. DEAL. Could I stop at that point just to ask a question, because it goes back to what Mr. Green had said earlier.

Are we seriously pursuing efforts now to tie in our trade agreements or other negotiated agreements with other countries their requirement that they clamp down on these matters internally? For example, it would seem to me that it is not too far-fetched to say that we would build into trade agreements that this kind of activity coming from another nation is an unfair trade practice that could

trigger sanctions in other areas if they don't do something about it and we can trace it to coming from their country.

Are any groups pursuing those kinds of arguments, to say that that is the only way we can ever really get a handle on it because of the international nature of the entity?

Mr. HANCOCK. Sir, I am not equipped to answer that question, so I will have to defer that to the other panelists.

Mr. SILVA. Well, I guess if you look at the spam problem individually, okay, I am not so sure that going after the people sending the spam is the answer as opposed to taking the site away that they are being directed to. Okay. The spam is usually, in many cases, directing to a Web site. It really doesn't matter who sent the mail. It really doesn't. The fact of the matter is that all of the spam is directing someone to a Web site. Take the Web site away, and the spam is meaningless anyway, and the purpose of sending it ceases to exist.

So, you know, if we take sort of most of that away, then that takes the spam down a considerable amount, down to sort of the mail order fraud sorts of things and other things like that. So, go after sort of the originating source—or, I should say, the destination rather than the source of the spam, okay, because where the spam comes from I think matters not, and people will just come up with more creative ways of hiding where it is coming from. Even if we have trade sanctions, our ability to be able to track them could become more difficult.

Mr. DEAL. Are current laws adequately directed in that fashion?

Mr. SILVA. Absolutely not.

Mr. HOLLEYMAN. Mr. Deal, if I may comment. When the President released in February this year the National Strategy to Secure Cyberspace, there is one section of that dealing with what we need to do internationally. One of the recommendations is to get more countries to join the Council of Europe Treaty on Cyber Crime. And so part of what we are doing, before we get to using trade sanctions, is holding out the type of models that we think are appropriate.

This new agreement that the U.S. reached with Japan was the first formal MOU, as I understand it, between governments. I think there is a huge opportunity for leadership.

And in response to the earlier question from Mr. Green, I think when you take a subset of this, which is spam, we do think that there is some appropriate legislation that could be useful that could then become a model for our trading partners. Clearly, none of this will be resolved overnight, but we should use every tool internationally. And I think there is a unique opportunity for U.S. leadership in this area, because the field is so fertile, and we are one of the handful of countries dealing with this in a serious, significant way.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. UPTON. Ms. McCarthy.

Ms. MCCARTHY. Thank you, Mr. Chairman. And thanks to the panel. And I did get to listen to Mr. Green and Mr. Deal's questioning, and I appreciate your forthright answers.

And so as we look to a solution—because each of you in your papers talk about in the end what can be done. I find repeating

themes of the trade agreements and education, international laws such as just mentioned by the President's recommendations in February, changes in software design, and incentives to infrastructure custodians, such as several of you represent, to help with research in this. And so I guess I would like to revisit with you how you would wish the Congress to proceed with any of these in sort of a sense of priorities given, you know, the skills and the abilities that we have.

All of these papers are fantastic and your ideas are great, but how—could you help us focus now on how best for us to proceed in this matter that will be effective, efficient, and timely with the resources that we have? Anyone. And all of you, if you wish to comment.

Again, I thank you for your thoughtful presentations and papers. They are outstanding.

Mr. HOLLEYMAN. Let me just mention a couple things. One, I think there is an opportunity on the law enforcement side as part of the appropriations process to make sure that U.S. law enforcement agencies have the right personnel, the right training, the right equipment to deal with this, and that we arm our allies—the U.S. personnel who deal with our international allies to help train those folks as part of an international effort.

I think second there is the effort by the U.S. Government to lead in terms of the U.S. Government's own attention to cybersecurity. The FSMA legislation that was passed last year has been a good model that we are now trying to deploy for the private sector. So we think that ensuring that Federal departments and agencies are also creating that culture of security is important.

And, finally, I think it is building this culture of awareness. And that is, using every platform to talk about this, to create this culture of security, getting information into the hands of your constituents; so whether they are a small business, an individual, a large business, they understand what part they have to play in this. And as an industry, we are eager to work with you in making that information known.

Ms. MCCARTHY. Thank you very much.

Mr. WONG. Ms. McCarthy, part of it I think is having to do with an awareness campaign, making small steps now to bigger gains and bigger goals.

I remember growing up, that when forest fires used to be a major problem, and we came up with the Smoky the Bear campaign. And since then, arguably, we have had less forest fires, except for recently in California.

When Mr. Green had asked earlier why do we still get so much spam, why are there so many attacks after these things have already been discovered, well, even a very simple awareness issue is that it has been estimated that more than 60 percent of the desktop computers out there do not either have antivirus software or updated antivirus software. So there is a big part of it that can be helped just by the awareness of having the right software or things that will detect some of these things that—the attacks that are coming.

The awareness certainly starts from children, also through businesses and adults and home users and employees, where we can

each actually secure our own individual piece of cyberspace, thus making all of cyberspace more secure. And that starts with education and awareness, and we can take those steps now.

Ms. MCCARTHY. Thank you, Mr. Wong.

Dr. Hancock.

Mr. HANCOCK. I would have to agree with the panelists. I would also state that I believe that awareness, as Mr. Silva mentioned before, has to start at a very early age. And I will give just a quick anecdotal example.

My oldest stepson is 32 years old and runs e-mail at one of the largest telcos now, and he has been around cybersecurity since age 11. My youngest son is 14; he has not known a day of his life without a computer around. And when he first started using the P-to-P-type of technology and copying music for free, we had to have a little lecture. But that sort of thing is very important, because by educating him, I found that he very quickly educated all his friends. And he runs around with about 10 or 12 kids that are very much into cyberspace. One of these children just makes amazing Web sites for businesses at age 14.

So I believe that early education in the K through 12 area is absolutely critical to going forward as a national plan.

Simultaneously, though, I believe that we also have to be aware that we are not out of the woods when it comes to terrorism. Terrorism is going to use technology now and in the future to go back and further their goals. So one of the things we have to also keep in mind is that while we want to have a long-term relationship with our youth and basically bring them up the right way and teach them about security, we also have to simultaneously remember that there are adults out there that are going to use our current open infrastructure against us. And in some ways it can be rather devastating. Because of that, I believe that there is also a need to jump some legislation and to jump into some areas that may be not as well thought out as we would like, but at least can start to curtail some of these activities that are out there and start looking at some of these issues.

Some technologies, such as a technique called steganography, are known to be used by the opposition. Steganography is where you take technology such as a Microsoft Word file, or take a drawing or perhaps an operational plan embedded into a graphic, post it on a Web site; someone else can download the graphic, it looks like a graphic, it feels like a graphic, but you are hiding the data within the graphic. And at that point you can extract operational orders, you can extract operational information. This type of activity goes on. That kind of activity has to stop. There are techniques out there right now such as polymorphic check songs using things such as cryptologic signatures that will stop that sort of thing from happening, to keep from using an open infrastructure in a negative way and by the terrorists either through viruses, worms, or other kinds of infestations like steganography.

So I think it is a dual-pole problem. I think there is a long-term awareness problem that we have to deal with, but I also believe that simultaneously we have got to do something about some of the short-term issues and start taking some action; otherwise, we are not going to get on top of this.

Ms. MCCARTHY. Thank you.

Mr. Silva?

Mr. SILVA. I agree with Mr. Wong, that I think the education part of it is sort of the no-brainer thing and the low-hanging fruit right off the bat, okay? We teach our children in schools how to use computers, but it is not currently part of the curriculum to teach them how to use them safely, okay? As parents and teachers, we teach our children how to cross the street safely, but we don't necessarily teach them how to cross the Internet safely. So to the extent that the Federal Government provides some funding assistance to some schools, it would probably be worthwhile to direct some of that funding in the proper direction.

Another thing I think that is very important is the Department of Homeland Security is very interested in developing an early warning system.

Ms. MCCARTHY. Yes.

Mr. SILVA. And I think that Congress should support that wholeheartedly with as much vigor as is possible.

Now, with respect to—there always seems to be this sort of come back to let us just write better software kind of thing. I think that is sort of beating a dead horse, and I think it is a no-win game, quite frankly. But as I am sure Mr. Holleyman would agree, while we have a number of antivirus solutions that need to be updated on a regular basis so registered users do update them on a regular basis, people who run Microsoft Windows, for example, the patches are available on a regular basis. The problem is that a large number of computers—and it is a shockingly large number of computers—are running software which is not registered software and was not legitimately acquired, so therefore not entitled to all of the updates, patches, et cetera. So we are still looking at a huge number of machines that even if properly—if the software manufacturers properly produce the patches, et cetera, there are still a huge number of computers that can't get those patches. So it is still a big target for anyone to hit.

So just to close, I do believe that the education early warning systems are two very low-hanging pieces of fruit that I think we should dive right into.

Ms. MCCARTHY. Thank you, Mr. Silva.

Mr. PETHIA. Let me be the contrarian for a moment. I agree that awareness and training are going to be important and we should certainly pay some attention there. But the probability that we can drag 150 million users up that learning curve in a short period of time I think is pretty small, especially when you think about this as an international issue. If we want to protect ourselves from getting spam attacks, we have to educate the planet, not just the people in the United States. So that is a huge, huge drop.

I like to look for leverage points, and one of the leverage points I happen to think is possible in the short term—short term being over the next 5 years—is better software. I don't think the horse is quite dead. I think we can have better horses out there in our operating systems and our applications software and our networking software. It will never be perfect. We can't rely on that as a silver bullet. But I think the government has an opportunity through its acquisition practices to provide incentives to people who

produce products that reduce the overall cost of ownership of those products. And if you save money because you buy product X over your experience with product Y, reward the vendor with some piece of that savings.

The other thing is, as Ken mentioned, the early warning system I do think is critically important. Being able to develop an international indications and warning system that gives us advanced notice of these attacks is going to be critical to deal effectively with them effectively. And then ensuring that the various organizations that do research and development funding in this area within the Department of Defense organizations like DARPA, the Homeland Security Advanced Research Projects Agency, the Infrastructure Assurance and Infrastructure Protection Division of DHS, to ensure that those kinds of organizations continue to have a component of their budget that is focused on cybersecurity research.

Ms. MCCARTHY. Excellent.

Mr. Chairman, I apologize for going beyond my time, but I felt this would be worthwhile to have a summary from each on this question. I thank you.

Mr. UPTON. Thank you.

Ms. Bono.

Mrs. BONO. Thank you, Mr. Chairman. And thank all of the panelists as well.

It is a perfect segue in to me when you started talking about children, because I have two teenagers at home and I have tried to educate them. We have talked about viruses, worms, and spam. But 1 day on my PC, this wonderful little Bonzi Buddy came up, which brings us to a new area, and that is Addware and Spyware. And nobody has really talked about Addware and Spyware yet, but I consider them to be as big a burden and if not increasingly more threatening to PC owners, both businesses and private individuals, as certainly spam is.

I think people aren't quite aware of Spyware and Addware, but I try to describe it to my colleagues as the guy following you around in the trench coat with glasses on that you don't know is there but he is monitoring your every move. And I am wondering if you all—to be quite honest, I have legislation on Spyware and Addware out here, so I am hoping you all will lend some testimony to support my cause, although this is more about viruses.

But if any of you could comment briefly on whether you think Spyware and Addware is as big a threat as are viruses to PC users. And, Mr. Wong, I am a huge Symantec user, and appreciate the work you do to save my family from harmful attacks.

Mr. WONG. Well, thank you very much.

Well, in terms of Spyware and Addware, that is an increasingly large—that is an increasingly large problem. I think it is even worse than you have already said it, in terms of having someone follow you around. In some cases, it is as bad as having someone in your own home and hiding in your closet without you knowing it. There are many technologies that are currently available that help block Addware and Spyware so that you can prevent some of these things.

We certainly support the kind of legislation that you are talking about. But the other thing to note is that there is something called

Spyware that can be used for good purposes as well, when you need to monitor, when you need to manage or help administer computers remotely, say if you need to support other people who work in your environment. There are certainly useful and legitimate reasons for having things or software that sit resident on a desktop and help you manage or monitor it.

It becomes a problem when these things are in stealth mode, when they are hidden from the intended target, and when they are used for malicious purposes sometimes, as many times they are.

Mrs. BONO. Excuse me. Let me jump in here. What is so great about my legislation, Mr. Chairman, is that all we are asking is that somebody who is placing some Spyware or Addware on an end user, is that in the end user license agreement they state we are doing this to you and you need to know it. It is a single box, and here it is, and do you accept it? And you can check yes or no. Because I see some reasonable reasons also for Spyware, Addware. It could be a consumer-friendly shopping service as well. But also, at the end I would like to have a one-button removal tool that removes the Spyware or Addware.

So I just wanted to say that hopefully we are in agreement on this. And I believe BSA has been supportive of my legislation.

So does anybody else want to comment on Spyware or—did I cut you off, Mr. Wong? I am sorry. Go ahead.

Mr. WONG. No, not at all. Certainly having a button to remove it is something that would be helpful. There is already technology that can help block that kind of behavior and that kind of software that comes out. It is also worth mentioning that, in addition to having someone monitor your computer through Spyware, that through worms and viruses that are related, people who—these hackers can deposit code on your systems to gather information from you. And we have seen much of that before, where you inadvertently give passwords out to financial bank accounts, passwords to trading accounts. We have seen worms out there and viruses where they actually harvest information from financial institutions. If you are X bank or this financial institution, then send this type of information to another computer so that we can see—so that they can see what is in there and use it for their own malicious intent. But we fully support your type of initiative.

Mrs. BONO. Thank you.

Yes?

Mr. SILVA. I think that the initiative is very good. I think it is exactly the right direction for Spyware and other things. In fact, I mean, I believe that for any software that is installed on a computer, the user should know what they are installing, okay, quite frankly.

Again, the problem comes back to what we have already discussed earlier. This is a fine step for the United States to take, but again it could potentially become an international problem. Where, you know, your legislation would certainly apply and I think is a noble effort within the United States, and I think that is probably where we are going to go after the vast majority of it anyway, but I still think we have the problem with the offshore.

Mrs. BONO. I agree with you. But the initial reason behind my seeking this idea out was that when kids really download Kazaa

and these P-to-P-type programs, what they don't realize is there still is an economic model as the basis for it, but someone else is making the money, not necessarily song writers. But there still is a money-making motive behind it all.

So, yes, I think as Mr. Green said, it is a step in the right direction, and certainly if they move offshore. But currently it is the Kazaa sites and the P-to-P sites that are installing this Addware. I have had to go to the length of buying a computer for each of my kids to get them off of mine, because they slow the machine down and put all these great things on that are, you know, temperatures and times and you name it. So it is a step in the right direction, I think.

Mr. SILVA. So I think that maybe this is the first step in a multistep effort that, you know, perhaps in another year that we could actually have some legislation that actually targets the description for any software that, you know, that it shouldn't do things that it doesn't tell the user about. Okay? There shouldn't be software on a machine that sends data around and whatnot. Even if it is for legitimate purposes, the user should know, has the right to know what the software is doing.

Now, you know, I mean, there is probably some limits on that information. But, quite frankly, I think that your proposed legislation here is applicable in many areas, not just in Spyware. There is legitimate software that some people call Spyware.

Mrs. BONO. Well, thank you.

Thank you, Mr. Chairman.

Mr. UPTON. Mr. Bass.

Mr. BASS. Thank you, Mr. Chairman. It is a great hearing, very interesting.

In the committee memo here that we were given today, I would like to read a sentence and then have some comments from you.

I quote: The main reason for the long life of viruses and worms—and I suppose this has also occurred for the prevalence of viruses and worms—is a lack of updated antivirus protection by system administrators and computer users.

I know you all have addressed this issue in some detail already. Is it time for the Federal Government to establish some sort of an Internet security agency that would develop standards for all legitimate software, require automatic updates, patches, and so forth, and establish a base level for every single computer in the country regardless of whether the user knew or didn't know what was best for that particular unit to prevent the spread of viruses and worms?

Anybody want to comment on that?

Mr. HOLLEYMAN. I will start.

I think, Mr. Bass, the question you are asking is an appropriate question, which is, what does it take to build this culture of security? And it requires different things for different types of users. I mean, there are different standards we can rightfully expect for a home user, for a small business, for a large enterprise. We need to have different standards that address that. I am not sure that a Federal agency at this point is necessary to do that, given the new tools that are being placed within DHS giving some of those State

Departments an international role. I think we have the right resources there.

What we just need to do is build this awareness of how often does an individual need to update their antivirus; what would you expect within a medium-sized enterprise; do you have a firewall in place? Make that information plainly available, and then ultimately there is a balance that has to be struck here. We could create software, we could create a network that is so secure that it would be very difficult for legitimate users to use. You could build so many locks in a house and a building that people couldn't get in there. And so the balance has to be we have to improve on the status quo, because that is not acceptable. At the same time, we need a reasonable balance so that you have don't have to be a technical expert to run your home computer or your office computer. You just need to know what—

Mr. BASS. And I know others may want to respond to this, but is there any reason why any computer in this country shouldn't have some kind of antivirus software on it as a requirement?

Mr. WONG. Mr. Bass, there is no reason why there is a computer system out there that shouldn't have antivirus software on it.

Mr. UPTON. Mr. Wong, if I may just interrupt. You know, at Rotary you would be fined a dollar for that. You can at least mention Norton, right?

Mr. SILVA. Okay. So, actually the problem is these are called personal computers, a lot of them; and personal computers mean that they are shaped based on the personal characteristics of the individual who uses them. So I think that what you are proposing is tantamount to trimming a little fat off the Constitution. I am not so sure that if we have a bunch of computers out there, that the Federal Government is going to require them to receive automatic updates from somebody; who do they trust? Is this the government that they are going to trust to provide these updates to them? Or who is going to provide the updates to them and they must trust them?

And the other thing is I think that the public outcry in this particular area of having software installed without the knowledge of the user—you know, on their systems as a mandate, I think would just be—I mean, it would just be shocking how—the public outcry on this.

Now, I mean, personally I think that we should—that smart computer users would in fact update their software and have it, but I am just not sure that any kind of agency, you know, Federal agency that required automatic updates on people's computers for all of their software is something that the public would tolerate, quite frankly.

Mr. HANCOCK. I would like to address both issues. One issue, having to do with should you have a baseline security of your system. One of the things that I have been involved in for the last 2 years is the creation of cybersecurity best practices for the telco industry. And that is where anytime you pick up the phone, the person at the other end that runs all that for you, it is those kind of companies. Prior to 2 years ago, there were no cybersecurity best practices at all; now there is over 200 of them. Those best practices include virus protection, they include a wide range of security

issues involved. There is a lot more to it than just should we go back and compel people to have an antivirus capability or firewall, or whatever the case may be.

The problem with that is that the best practices are a start, they are not a finish at any stretch, and we are continuing to refine those. The Internet security lines, we have also generated best practices both for the home user—there is a document about that—and best practices for executives on how to go back and measure their organizations, saying are we doing the right thing security-wise. Those are a start. They are not mandated, so to speak, but they are a very strong start to get people to start being aware of these are the things you can do.

There are standards and practices that are put out by experts. The members of the team at the SEC, for instance, are all my equivalent partners; at the phone companies, are all the chief security officers of all the different phone companies that are out there, and they deal with the same problems that I do.

But that is where we are starting right now because the problem is, is that when you really get down to it, personal computing, while we all use it and we all have it, is one aspect of computing. There is an aspect where a, quote unquote, personal computer may be used in a process control environment to control a factory automation network; where, if you put any antivirus software on there at all, or mandated it all, you would actually take that computer and make that invaluable to a desktop but it doesn't work at all in a factory production floor. The same thing would apply in power companies or water treatment facilities for the water plants. And I have a vast amount of experience putting these kinds of computers in, and none of these would be appropriate for antiviral-type of operations.

However, we can confront those types of networks with different types of security technology to keep that sort of thing from even hitting those networks, because those computer networks, if they were forced to have that kind of technology imposed on them, would never operate efficiently nor operate correctly, and the end result is certain infrastructure would go splat and not work at all.

So I believe that under certain categories there is a good security baseline requirement. I think there has been an enormous amount of energy put into the generation of real best practices that have real capabilities in the last 2 years that didn't exist 2 years ago. But I simultaneously believe that a mandate of a base security configuration for all computing types would probably be problematic at best, and something dangerous at worst, under certain conditions.

As far as a Federal agency for mandating an oversight of something like this, I don't know that it is quite the time for that just yet, but I do believe that the adoption by the Federal Government of best practices and standards for computational capabilities such as those that are being developed by NIST right now and those developed by the Department of Commerce and those developed by the SEC, and start to spread those around where it is uniformly applied. And then also making that part of the chain of trust agreement between the Federal agencies and whoever they purchase equipment and technology from would be a very strong start to start making some of that stuff happen.

Mr. BASS. Thank you, Mr. Chairman.

Mr. UPTON. Thank you.

I would like to go back to something that Ms. Bono said, frustration that she had with her kids that she actually had to purchase a computer for each one of her kids. And I sense it was because of the P-to-P networking and the ability of harmful worms and viruses to spread, because she didn't have three computers—two kids. Right? How—

Mrs. BONO. Excuse me, Mr. Chairman. Four computers. My husband has his own, too, because he is as bad as the kids.

Mr. UPTON. How do these P-to-P networks contribute to the ability of harmful worms and viruses spreading the damage? Is it an enormous problem? Is it a small problem? Does every family with kids need to get their own system for each one?

Mr. HANCOCK. Mr. Chairman, I can address it from my perspective. We have several hundred thousand customers on our networks, that probably there are anywhere from 80 to 90 million users. So we see P-to-P all the time. And the problem is that a lot of the end sources of P-to-P contribute false documents, false programs, things like that. Sometimes as a prank by children. Many times it is a way for them to go back and forward their agenda, like I said before, with the hacking gangs. We have actually had some situations like that.

In the situation of using P-to-P to go back and forth, it is just another mechanism to transmit a virus or a worm, no different than using e-mail or using spam to go back and using e-mail as a transport mechanism. So P-to-P is just another transport mechanism to move malware around. The difference is that most P-to-P is available to younger generation individuals, and those younger generation individuals a lot of times start messing around with this stuff and they don't know what they are messing around with. Or they actually have—in some cases we have seen rival cyber gangs, for lack of a better definition, that actually start to pick on each other by using P-to-P to transmit malware back and forth between each other, and it ends up getting spread all over the place because they put it up on different places for people to download things.

And that is my direct experience with that. The other panelists may have a different view of it, but that is a lot of the times how this stuff gets into place, is based upon what we see in a live network.

Mr. UPTON. And as you talked earlier in your testimony about the nightmare scenario about how viruses could get worse, spreading to DVD players, Xbox games, cable systems. If it is P-to-P, I mean, it would be pretty dramatic.

Mr. SILVA. Well, that is right. And I agree with everything that Dr. Hancock said. The thing that actually further complicates it is that a lot of the people who are using the P-to-P are doing stuff they shouldn't be doing. So their motives for reporting whenever they get viruses or worms from a P-to-P network are probably—there is probably a deterrent for them to report it, because then it begs the question, what exactly were you doing?

Mr. UPTON. Mr. Wong, I have a question. I will confess that I have your competitor antivirus on my system and I have had a little problem the last couple weeks. I would just be curious to know

how this is dealt with. When I turn on my computer, I have Microsoft XP, and when I am just about to ready to get logged on to my password, it all of a sudden goes blank. The whole computer shuts off. I have got to restart the whole thing; it takes a couple of minutes. It happens probably every week. And then there is a little notice that comes on that says, Do you want this report to be filed with—I think it is McAfee, but I don't know if it goes to McAfee or if it goes to AOL. And I hit and click yes, and watch the little bars go, and a minute later it says okay, and you go ahead.

What actually happens? How is that—is it reported that I had a problem? Is there some patch that I am able to get down the road that is going to fix it? Is this a ruse so that the culprit who sent this thing to me is laughing all the way? I mean, what is happening when I hit that yes button?

Mr. WONG. Well, Mr. Upton, you are using a competitor's software. I am not surprised. But that being said, there is a good likelihood that you probably even have a virus on your computer system right now.

Mr. UPTON. That is what I suspect.

Mr. WONG. When you press that button—and we have similar technology at Symantec where our 120 million users do have the ability to send us a sample of their virus that they may have contracted. When they send that to us, we have the ability to—if it is a new type of virus or a new strain, we have the ability to create an antivirus for it and then send it out back to that person who sent us that particular virus. And then we have the ability to then inoculate and send the benefits or the signature of that virus back out to our 120 million users so that they as well are protected.

Mr. UPTON. So that at some point when you get an update, it may be taken care of.

Mr. WONG. Absolutely, that is the case. We can see right now where even in our own antivirus laboratories we get as many as 10,000 submissions on a monthly basis of new viruses or new virus strains that have not been propagated in the wild. And what happens is that we develop definitions to detect these new viruses that you may not have even seen yet, and then you have the ability to, when you use the Norton antivirus product or Symantec, you get that automatically updated and sent to you without you even knowing it.

Mr. HANCOCK. Mr. Chairman, being the geek on the panel, may I suggest, sir, that you go to the NAI site and download a utility called Stinger, and it will get rid of that.

Mr. UPTON. Okay. Good. I will do that. Thank you.

Ms. Bono, you have additional questions?

Mrs. BONO. Thank you, Mr. Chairman. Thank you. Just a couple.

First of all, a comment that I think the ISPs are the first line of defense for the average consumer when AOL and MSN, or whomever, warns the user and reminds them to update. And I think for the average American the ISP is the portal to the Internet. They are not directly accessing the Internet. And so I would say that I think AOL does a good job, even though they use your competitor—I use, as I said, Norton. And I am a huge fan because I have gone—although sometimes you guys, your processes are

very, very elaborate and you could simplify them for removing a virus.

But would it ever get to the point where we have to just entirely separate our financial networks where—because that is my concern. I do all of my banking on line. And would you ever have an entirely separate way of accessing, say, your bank, and then keep your e-mail entirely separate? Is that where we are going to?

Mr. WONG. Well, I think it is a matter of functionality versus security. And to have something that is completely secure, you would have to completely separate it. But then, of course, it might not be functional. You might not be able to do the things that you really need to do to be able to communicate or conduct transactions that you might really need to do if you were fully, fully secured by having separate systems.

Now, that being said, what we can do is increase the level of protection that we have when we have sensitive information that we have on a single system, so that we have measures to protect us, to monitor things, to block certain behaviors, to block certain attacks that are coming in, to block viruses that are coming in, and to not let offending viruses or attacks come out of your own systems.

So I think that it is more of a solution of instead of let us separate it and not have the functionality that we need, we need to really concentrate on what can we do better to secure what we have so that we continue to have the functionality and the communications that we need.

Mrs. BONO. But in a strange way, if you do your banking over the telephone, using the keypad, it is secure. But the minute you go to your PC, you are losing that? You are not secure over the phone lines? No?

Mr. WONG. I wouldn't say that you are any more secure by using the telephone. There has been a lot of—there was telephone hacking before there was Internet hacking. And certainly you take the same type of risks in the telephone as you do over the Internet.

Mr. HANCOCK. And in some cases—I would agree with Mr. Wong—In some cases, one of the things you want to be careful about is making sure that you do what we call in the business “compartmentalization” of your own computer. Specifically, if you have things that are very sensitive, you would want to potentially encrypt those files or make those files where, even if somebody did get ahold of them, they are useless to anyone else.

And so you can't just assume that the computer is either secure or not secure. There are different levels you might impose upon yourself and on your own computer. So, for instance, on my computer I do my banking over the Internet; I charge and buy services over the Internet, but I am very careful who I do business with. I am very careful to use encrypted capabilities. I am very careful to store my data on my machine in such a manner that if you did break into my machine or someone did get onto my machine, if they steal really sensitive stuff, they are going to get a bunch of files full of gobbledygook because it has all been encrypted. So I think it is a matter of caring for different levels of sensitivity of information that you have and using the proper tools for that.

Mrs. BONO. Does adding a router protect you to Trojan horses?

Mr. HANCOCK. No, ma'am. Not at all.

Mr. PETHIA. And just building on that, we are almost talking about things like viruses and worms as if they were acts of nature that we can't do anything about. I mean, this is an engineering problem. And the reason that we are connecting everything with everything else is because it leads to greater business opportunity, it leads to greater efficiency, it leads to higher levels of productivity. There are good reasons to have all these things interconnected.

But what we need to do is to ensure that the engineering solutions that we bring to the table when we do interconnect these things come with the right security characteristics. And that is what I think we need to push for. Not go backwards and try to segregate everything, but rather to try to put things together in the way that we are to begin with.

Mrs. BONO. Interestingly enough, I think technology and the way we go is we move forward and sometimes we move backwards. Cell phones are getting bigger once again. So my thinking was, if we are going to start moving backwards again with separating out our networks.

But thank you, Mr. Chairman, for this second round of questions. Thank you very much.

Mr. UPTON. Mr. Bass, do you have further questions?

Mr. BASS. Thank you, Mr. Chairman. Yes.

I would like to address the issue of economic terrorism over the Internet. I know some of you alluded to it. In some respects, you could say that the attack on the World Trade Center was the equivalent of a declaration of economic war and the fatalities were people who were capitalists and in business.

The same kind of attacks can occur, as you all well know, over the Internet. And I was wondering if you could give me some sort of a summary as to the level and seriousness of organized international economic terrorist attacks on American or international Web sites such as Bank of America, for example, or a big international clearinghouse for funds and currencies, banking centers and investment centers and other economic spots. Is this a serious international problem? And what is being done about it?

Mr. HANCOCK. I will take it first. The answer is, yes. And definitively, yes.

Mr. BASS. And also are there governments that are conducting these attacks, or are these extranational forces?

Mr. HANCOCK. I can't answer that question directly, sir, and it would probably be inappropriate to do it here. However, I will answer the first part, and basically state categorically that more and more financial institutions are using the Internet or the equivalent thereof to actually become the financial clearing and transaction network that is being used by those financial institutions. In fact, there are a couple of major financial institutions just recently used Internet-only for their entire transactional load in a specific day.

In the case of January 25, when Slammer hit the Internet, that particular worm that hit the Internet was something that attacked a vulnerability that existed in a data base that had been patched 7 months previously. However, several large and major financial transaction institutions got hit very, very hard by that. And the

only thing that saved them from getting into a situation where they could not complete the required and federally mandated transaction clearing was the fact that it hit on a weekend.

Mr. BASS. Do you feel they were the target of the whole effort, or were they just a—

Mr. HANCOCK. They were there, and they didn't patch and they got hit.

Mr. BASS. I am interested in efforts that are made that are specifically organized to bring down economic institutions in the United States.

Mr. HANCOCK. There are attacks that I have seen that have been directed specifically toward financial institutions in the United States. Some of those attacks have been originated outside the United States, some have been originated by disgruntled people inside the United States. And those have been led through the Internet. In most cases, it hasn't been debilitating to the financial institution because the institution itself does all its back-end financials on a back-end network and not on the Internet or through a Web site.

However, that is changing because more and more are starting to go that way, and therefore a debilitating attack would have a severe financial impact on that institution.

Mr. WONG. Mr. Bass, if you take a look at the Bugbear virus, specifically that was actually targeted partially at financial institutions, where it was harvesting and gathering information and doing certain things if you were—a listed number of financial institutions that they specifically listed in the code of that particular virus.

Mr. SILVA. I think probably the U.S. intelligence services would probably be the best place to provide information on where—you know, asserted efforts against our financial community from foreign governments.

However, what I would like to point out is that in all the sort of worms we have been talking about today in a general sense, most of them—most of them were nondestructive in nature in terms of the data that they destroyed behind them. Okay? In other words, they didn't. They simply infected a machine and then went on to the other machine. In most cases, I am not saying in all.

If worms such as So Big, Blaster, NAGEE, and some of the others had actually—or in particular Slammer, which was specifically targeted at SQL data bases, MSSQL data bases. If those had actually eaten away and taken the data with them, that could have been very catastrophic. Many financial institutions in fact were infected with these worms, but it was nonimpacting to the customers because no data was altered or deleted. So it is not a giant leap to take these worms and make them some sort of targeted economic bomb, if you will. Fortunately, that hasn't happened yet.

Mr. WONG. I would take that one step further in that I completely agree with Mr. Silva, in that the worms and viruses that we have seen in the last number of years, they have been destructive in the sense that they have caused downtime and things like that. But we haven't seen deadly payloads. We haven't seen hard drive crashes. We haven't seen destruction of data. But that technology already exists.

There have been viruses that have been developed in the past where you can destroy the hard drive when you contract the virus, you can corrupt the data that is on that particular computer system. The worms that we have seen could be potentially just merely payload delivery devices for these types of destructive payload that already exists. So we haven't seen it yet, but the technology already exists, and that is certainly something that we need to be aware of for the future.

Mr. HANCOCK. I would agree with Mr. Wong and Mr. Silva both, and add on one last thing about that. Just the Slammer worm itself was a good example of rapid propagation and rapid consumption of Internet bandwidth with zero payload. And that was the thing that was very startling about it. It was very professionally written, it had a very high rate of propagation speed, like in the order of 42 milliseconds. But what is more important, though, is that the payload was nothing. And if you put in even a DOS command like format, space, C, colon, it would have been absolutely catastrophically devastating to an enormous number of machines.

So—and in the situation of taking and creating what we call a hybrid worm, which is a rapid propagation worm with a viral payload, is that possible? The answer is absolutely, yes, and it is just a matter of time.

Mr. SILVA. I guess I want to make sure that we are not sort of going in a direction where we are sort of suggesting that doing business on the Internet is a questionable thing, because I don't think it is. In fact, I think e-commerce on the Internet is very safe because there is fair amount of authentication that goes on between the bank and the end user here. Okay?

So in terms of how these things move around and whether or not your credit card information is safe, I would absolutely say that credit card information that is passed over an SSO connection is far safer than pin numbers entered on a cordless phone in your living room.

Mr. BASS. Thank you, Mr. Chairman. I might want to follow up on that if there is a chance for one more follow-up round. Thank you.

Mr. UPTON. Well, gentlemen, I thank you very much and we all appreciate your testimony, your leadership on this issue. It is a mighty concern by all Americans at all levels of use on computers, whether they be a small business, a large business, or our homes and working with our kids and our husband and wives. And we appreciate your leadership and your commitment to the cause, and we look forward to hearing from you again. Thank you very much. God bless.

Whereupon, at 11:29 a.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]



November 10, 2003

Honorable W.J. "Billy" Tauzin
2183 Rayburn House Office Building
Washington, DC 20515

via: email and US Mail

Re: Subcommittee on Telecommunications and the Internet

Dear Mr. Chairman:

Per the request of Garret Graves we are submitting this overview of the issues surrounding vendor responsibility. As outlined by our CTO James Stickleby.

Should you need any questions answered please feel to contact us at 225-612-2121.

Sincerely,

Pete Stewart
CEO
TraceSecurity, Inc.

Cc:
Garret Graves, Assistant Chief of Staff for Billy Tauzin

TraceSecurity, Inc.
7117 Florida Blvd
Baton Rouge, LA 70806
225-612-2121 Phone
225-218-0101 Fax
www.tracesecurity.com



Vendor Responsibility

For the Subcommittee on Telecommunications and the Internet
Jim Stickley, CTO TraceSecurity
November 2003

Problem Defined

Federal, State and Local Government Institutions as well as corporations rely on public announcements from vendors, security firms and other public forums to receive critical information about security vulnerabilities in software running on their systems. Unfortunately, over the past several years, it has become evident that some manufacturers would rather cover up vulnerabilities than tarnish their reputation by making them public.

Proper Etiquette

When a new vulnerability is discovered and reported to the corporation that originally wrote and currently maintain that particular application, there are generic rules that are expected to be followed by all involved. These rules, though not mandated by any specific law, guide all parties involved in proper response, resolution and ultimately public notification. When a new vulnerability is discovered, the individual or corporation that discovers the vulnerability will contact the corporation of the software and give detailed information about the issue. This information is generally very detailed in nature to help guide the corporation directly to the source of the problem. Sometimes, proof of concept code is supplied at the time of disclosure to further explain the vulnerability and potential threat level. It is understood by all parties involved that this information will not be released to the general public until the corporation has had sufficient time to review the issue(s) and create a patch or workaround to the problem. The term "sufficient time" is vague but is generally understood to be a maximum of 30 days from notification to public announcement. The time will vary depending on the corporation's response or lack thereof. When followed properly, this system works well. The corporation can resolve the issue before the mainstream public and possible hackers and or cyber-terrorists are made aware that the issue exists. When the public is notified, the announcement states the threat clearly, including possible consequences if this issue were to be exploited. In addition, relevant patch information is often included in this announcement. In the event that the corporation chooses not to resolve the issue, the public is still notified with a warning that the issue exists and of potential consequences if the issue were to be exploited. It is then left up to the public to create its own solution to the issue or disable the affected service.



Corporate Legal Maneuvering

It is rare that a corporation will want to notify the public about a vulnerability related to its product or service, but they understand the security risks that the users of its products would face if they did not. Unfortunately, some corporations have preferred not let the public know of any such vulnerabilities and are going to great lengths to make sure these issues remain a secret and are buried where no one can find them. The most commonly used tactic is the threat of legal action. When the corporation is notified of an issue, rather than resolve the issue and notify the public, the corporation will respond back to the company or individual that originally discovered the vulnerability and inform them if the problem is made public, the corporation will have no choice but to pursue legal remedies available to them. The threats vary and there is always some reason why they feel this is acceptable behavior. In some cases the corporation will take matters to the next level and start contacting other companies that may have been involved during testing when the vulnerability was discovered and threaten them with legal action as well if this information is released. By using this tactic, the corporation generally can cause enough concern to all parties involved, causing the matter to be dropped rather than risk any legal action. In these cases the corporation may still create a patch to resolve the issue, though no public disclosure is made available about the security ramifications.

Public Disclosure

Because new patches are released by corporations almost daily, it is difficult for the public to know which patches are truly important. Because of this, most staff and diligent home users watch for public notices about security related patches. Several organizations offer patch services based on security related patches and there are a number of email lists that users can subscribe to that give out information about new vulnerabilities and where the security patch can be found. If a patch is released that is not listed as a fix to a security issue, it will be overlooked by the majority of these services and therefore will not be resolved by those who are looking to these services for guidance.

In addition, corporations do not apply all patches released. Mission critical servers for example (generally the systems that house the confidential data such as banking information, credit card numbers, sales transactions, etc.) are too critical to daily operations to risk applying a non-critical patch. Firewalls, routers, switches and other infrastructure on the corporate network are also seen as mission critical and must maintain 99.9% up time. If a patch is released for any of these systems and is not seen as a critical security related patch, in most cases it will not be applied. The theory of "if it isn't broke, don't fix it," plays in perfectly here. In many cases, when a non-critical patch is released and applied it can cause issues in other



parts of the system and ultimately take servers off-line. This has caused many administrators to be very hesitant about applying any new patches unless absolutely necessary.

When an organization releases a patch and does not mention the security ramifications, it is guaranteeing that a large percentage of corporations in the US will not apply the patch with any urgency. As a result, critical systems are left exposed and vulnerable, unbeknownst to system administrators.

Industry Examples

As an example, in the past we notified a corporation that markets a firewall as never having a single vulnerability, about two separate vulnerabilities. One vulnerability allowed anyone on the Internet to gain access to the firewall and take control of it. The second vulnerability would allow anyone behind the firewall (on the internal network) to gain access to the firewall and take control of it. Both of these vulnerabilities would be seen as major issues to the public. The corporation responded that they had recently released a patch update for the product which would resolve the issues. The patch update was for various product enhancements and made no mention of security issues in the product. Notification was made to the corporation that an advisory would be sent to the public to encourage them to apply this patch due to the security issues, their attorneys immediately made contact and warned of serious legal ramifications if the issues were disclosed and published. To this day there is no mention of these major vulnerabilities. The company continues to advertise that they have never had a vulnerability.

In another instance, TraceSecurity informed a corporation that offers an online banking application that is used by hundreds of banks throughout the United States of a security vulnerability. This issue could allow anyone with hacking knowledge to gain user names and passwords to online banking accounts of banks that use this application. The company made no real effort to respond to the issue for several weeks. Finally, after feeling the company was making no effort to resolve the issues, we notified them that the banking industry would be made aware of the issues through a press release by our company.

At that point TraceSecurity was called and informed that legal action would be taken if this information was given out to anyone in the public, including anyone in the banking industry. This corporation subsequently contacted the bank who had originally hired us to test for potential security flaws on their network. The bank was told there could be legal action against them as well if my company released this information. This issue has not been completely resolved at the time of writing this document, though the corporation has been aware of the problem for over a month at the time of this writing.

TraceSecurity, Inc.
7117 Florida Blvd
Baton Rouge, LA 70806
225-612-2121 Phone
225-218-0101 Fax
www.tracesecurity.com

**Conclusion**

Cyber-crime and cyber-terrorism cannot be reduced or eliminated when corporations are free to hide major security issues from a public that uses their software. Because of the legal cost many companies such as ours do not want to endure a legal battle with a corporation and therefore are left to allow these issues to go undetected and unprotected by most. In a time when the United States is trying to stay one step ahead of Cyber-crime, it is dangerous and reckless that corporations such as these are using the legal system and other strong hand tactics to prevent the distribution of necessary security warnings to a poorly informed public.