CYBER SECURITY: PRIVATE-SECTOR EFFORTS ADDRESSING CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 15, 2001

Serial No. 107–74

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
76–310PS WASHINGTON : 2002

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

COMMITTEE ON ENERGY AND COMMERCE

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

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

CYBER SECURITY: PRIVATE-SECTOR EFFORTS ADDRESSING CYBER THREATS

THURSDAY, NOVEMBER 15, 2001

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

The subcommittee met, pursuant to notice, at 1 p.m., in room 2322, Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Shimkus, Terry, DeGette, Doyle, Harman, and Markey.

Also present: Representative McCarthy.

Staff present: Ramsen Betfarhad, majority counsel; Jon Tripp, deputy communications director; Mike O'Rielly, majority professional staff; Brendan Williams, legislative clerk; and Bruce M. Gwinn, minority counsel.

Mr. STEARNS. Good afternoon. And welcome to the Subcommittee on Commerce, Trade, and Consumer Protection hearing on cyber security.

You're welcome to sit down.

I'm pleased that we are joined today by a group of distinguished witnesses and look forward to hearing their testimony. The witnesses today collectively represent the best minds on the issue of cyber security, and I'm confident they will help us better understand the issue and its increasing significance.

In the aftermath of the tragic events of September 11 we as a Nation, it seems, have become obsessed with security, and that is understandable. So it is also understandable that our hearing today will also be colored to some extent by the events of September 11 and new worries over cyber terrorism. Still I do want to emphasize that the problems that gave rise to cyber security concerns predate September 11 and cyber terrorism worries.

Most important, those problems have begun to increase in sheer numbers and magnitude in an alarming rate. Let me explain.

In just over a year as a result of only three cyber attacks, the I Love You, Code Red viruses and February 2000 denial of service attacks in excess of $10 billion was lost.

The number of cyber attacks as reported by the Computer Emergency Response Team at Carnegie-Mellon University is expected to double this year from last year to some 40,000.

Now, a survey of 538 computer security professionals both within the government and private sector released this past March and

conducted by the Computer Security Institute with participation of the FBI's field office in San Francisco, found that 85 percent of the respondents said that they had detected computer security breaches between March 2000 and 2001. Some 58 percent of those respondents had detected 10 or more incidents of vandalism, theft of information, financial fraud and denial of service attacks.

Quite significantly, 64 percent of respondents had acknowledged financial losses due to cyber attacks or worse breaches of their information systems.

Cyber attacks and breaches of our Nation's information systems are especially worrisome when we realize that most aspect of our daily lives from the mundane to the profane, are touched either directly or indirectly by various information systems storing, processing and exchanging information via the electronic medium, the most visible of which is the Internet.

Just about everything we do involves the processing and exchanging of information electronically. Therefore, cyber threats to the Nation's information system, be they viruses, worms, denial of service attacks or something as yet not thought of must be taken very seriously.

If there are attacks yielding substantial breaches of our Nation's information systems, not only will we face staggering financial losses, we will also face more instances of tragic loss of lives.

As our information system infrastructure has become interoperatable, easy to access for sake of increasing efficiency and productivity, it has become more vulnerable to cyber attacks. The greater the degree of interconnection and interdependence between the various information systems, the higher the cost of disruption due to cyber attacks.

The Internet has tremendously accelerated this move toward increased interconnectivity and ease of access to information systems. And as such, the Internet connection to an information system containing mission critical information, such as financial data and intellectual property, has become a frequent point of cyber attacks.

The custodian of the Nation's information systems, the ones underpinning our economic welfare, is of course private industry. Companies large and small have historically made great strides in protecting their mission critical information operating systems. However, the cyber security challenges that they face have both increased in number and magnitude as the importance of information systems to our economic welfare has increased with the advent of the Internet.

We'll hear today that private industry is rising to these new challenges, but there still is more work to be done. For example, even though the horrific events of September 11, 2001 have put additional pressure on companies to reexamine their security procedures and practices, according to a recent poll of 150 chief information officers by CIO magazine, almost 40 percent of America's larger companies still do not have cyber security experts on staff or under contract. Cyber security measures cannot be an afterthought when designing, operating and managing mission critical information systems.

Since September 11, we have learned that terrorists do have the wherewithal to undertake the unexpected. Terrorists and their re-

cruits also have grown up in the digital age and thus, most probably, possess the technical skills to undertake concerted and effective cyber attacks. And as the real and virtual worlds have become more closely intertwined, cyber terrorism can potentially engender greater pain and tragedy, and thus become more attractive to unscrupulous terrorists.

I'll end by borrowing Ms. Davidson's most instructive words, "The price of cyber security, as with liberty, is eternal vigilance," and as we all know, freedom is not free.

With that, I'll turn to the ranking member of the committee, Ms. DeGette who is substituting for Mr. Towns.

Ms. DEGETTE. Thank you very much, Mr. Chairman. And thank you for holding this hearing.

In this time of uncertainty in our economy and in our country, these issues also face our business community. And I would echo very much of what the chairman talked about in terms of the integrity of our computer systems and our data in a time of terrorism, and the important role that private industry has to play in preserving the integrity of those systems so that we can preserve the integrity of our economy.

I would like to talk an issue not raised by the chairman, because I do concur with so many of his statements, and that's the issue of identity theft. This is an issue that we've talked about for many months in this subcommittee and which is even more essential today with the terrorists that we're facing.

An adequate cyber security in our commercial information system will increase the likelihood of identity theft. With the dawn of the information age companies collect, store and transmit large amounts of consumer information over computerized networks. Consumers rely on the security of these networks to protect personal data like Social Security numbers, unlisted telephone numbers, addresses, maiden names and information about their information.

As we have heard during previous hearings of this subcommittee, if this type of personal security is compromised, any of the information can be obtained and used to steal identities of unsuspecting Americans. Therefore, the security of commercial information networks concerns all consumers and is another aspect of the importance of cyber security.

Unfortunately—well, fortunately in one way but unfortunately in others, after September 11 we had thought that many of the hijackers of the airplanes on that day were using stolen identities. The fortunate thing was that in large part turned out to not be true, but yet stolen identifies were still used by some of terrorists in the September 11 attacks. At least one example that we know of was using the stolen identity of a deceased New Jersey woman in order to evade capture. And heaven knows how much this could happen in the future, and how difficult that would make apprehension by law enforcement agencies of suspected terrorists.

It is essential that both the private sector and government work to eliminate unauthorized access to personally identifiable information, which is the source of identity theft. Unauthorized access to the commercial information systems can be overcome with cooperation, and that's one reason I'm particularly looking forward to hear-

ing the testimony of our witnesses here today. Because as I've thought all along, this is not something that the government can work out in isolation, nor is it a problem that we should expect private industry to attack on its own.

Mr. Chairman, we need to continue to fight the war against cyber terrorism on all fronts, including identity theft. And I look forward to working with you and also the other members of the committee and hearing from our distinguished panelists on this issue.

And I yield back the balance of my time.

Mr. STEARNS. Thank you, gentlelady.

Mr. Shimkus from Illinois.

Mr. SHIMKUS. Thank you, Mr. Chairman. I want to thank you for holding this hearing, and you probably had mentioned to the panel, I'm glad to see you all here.

We have a lot on our plate today with our bioterrorism hearing downstairs, our conference has called an airport security briefing at 1:15 in AC5, and now this. So if we're running back and forth, let me apologize for myself and the rest of my colleagues.

Obviously, e-commerce and security are a big issue, and even with September 11 and the past, we will see an expediential growth, probably, in the use of facilities on electronic transactions.

I actually had a meeting yesterday morning with the Postal Service, and their projections are now outdated because of how people will rapidly move into their realm, which means if it's an easy target, terrorists will attack easy targets. And if it's disruption of our commerce and communication, and the like, that's another aspect.

So you all have been dealing with it in one way or the other. We know that you verified your threats, your vulnerabilities, and we would be interested in hearing what you're doing to protect yourselves and your clients.

I will end with saying I don't know of security because of Ms. DeGette's statements, I don't know if security is just a cost of doing business. I do believe that, darn right, there should be a value added aspect of having good control over your own data bases and in protecting security; that should be beneficial in some aspects depending upon your business. It probably should not be considered just a cost of doing business, but there's probably some very good value added aspects, and if that is properly promoted that people can take advantage of.

With that, Mr. Chairman, I think it's going to be a great hearing. I appreciate the panel being here. And be patient, we will get to you. Thank you.

Mr. STEARNS. I thank the gentleman.

The gentleman from Pennsylvania, Mr. Doyle.

Mr. DOYLE. Thank you, Mr. Chairman, for holding this important and timely hearing on cyber security.

The tragic events of September 11 demonstrate the willingness and capability of America's enemies to utilize modern communications mediums like the Internet and email to plan, organize and facilitate their attacks. And since that day we in Congress have examined a variety of proposals to strengthen and modernize both our domestic and international responses to terror.

Legislation is in the works to ensure the safety of imported food, improve the safety of our airports and enhance our enforcement and investigative capacities. I think it's only logical that Congress should address the possibility that future attacks could likely exploit vulnerabilities in our cyber security systems, both public and private.

Just as cyber security needs of essential government agencies such as the CIA and the Pentagon must be designed to prevent unwanted access to classified information, like intelligence directives and troop movements, private corporations need to ensure that personal information like Social Security or credit card numbers are not stolen by hackers looking to create false identities. After all, many of the hijackers on September 11 used fraudulent identification to carry out their evil business.

In what may be a glimpse of the future, it seems now that one Federal agency is taking a proactive approach toward cyber security. An article that appears in the current issue of Defense News highlights the Pentagon's efforts to fight back against hackers by creating an active defense network capable of tracking hacker attacks back to their origin while covertly monitoring the source of suspicious attacks. According to the article, the agency predicts over 40,000 attacks on military networks by year's end, a figure that's up from about 22,000 in the year 2000.

Back on my hometown of Pittsburgh we're fortunate to have one of America's greatest authorities or cyber security, the Center for Emergency Response Team or CERT of the Software Engineering Institute of Carnegie-Mellon University. CERT at SEI is a federally funded research and development center whose primary goals are to ensure that appropriate technology and systems management practice are used to resist attacks on network systems and limit damage and ensure continuity of critical services in spite of successful attacks.

The center is the first to respond to computer attacks, such as the recent Nimba and I Love You viruses. According to CERT statistics, nearly 22,000 incidents of security violations occurred last year with over 34,000 recorded already this year. Clearly incidents of cyber attacks are on the rise in both the public and private sectors.

I want to commend CERT and the Electronics Industry's Alliance for taking the initiative to form the Internet Security Alliance, a collaborative partnership that brings together industry and software experts to better address the growing need for timely, informative responses to cyber terrorism.

I look forward to hearing from Mr. Dave McCurdy, the President of EIA and the Executive Director of the Internet Security Alliance about the efforts of this new collaboration. Legislators to executive, to Internet security technicians; we could all stand to learn a great deal from the Internet Security Alliance.

As my colleagues are aware, this subcommittee has devoted a significant amount of time and resources aimed at providing members with a plethora of information relevant to online security measures and protection of personal information. We have listened to a range of testimony from experts who, in some instances, high-

lighted the need for strong protections guarding the access to and the unwanted use of personally identifiable information.

I hope that this committee will soon take action to bolster to e-commerce activities of both the public and private sectors.

Mr. Chairman, I thank you.

I yield back the balance of my time.

Mr. STEARNS. I thank the gentleman.

The gentleman from Georgia, Mr. Deal.

Mr. DEAL. Thank you, Mr. Chairman. Thank you for assembling this very impressive panel today, and I look forward to hearing your testimony.

Like Mr. Shimkus said, it is a busy time and we may have to apologize for people running in and out, but we do so in advance and I hope you will understand that.

It's a pleasure to see our former colleague, Mr. McCurdy. Nice to see you again, Dave.

Mr. Chairman, you know, I'm like a lot of people, I wish for a simpler time. When I read Future Shock many years ago, like many of you, we probably thought it was science fiction and would never come to be. Unfortunately, that rush of the information age has truly crashed down upon us.

I think of one of my colleagues in the General Assembly of Georgia who said that he lived in a small town, and to illustrate it was, he said it didn't even need turn signals on your car because everybody knew where you were supposed to be going and if you made the wrong turn, your wife would know about it before you got home anyway. We don't live in a world like that anymore.

Unfortunately our lives are very tangled and confused in terms of who has control over our lives and who has control over information that's pertinent to us. And the security of that information, of course, is what all of us are concerned about. And it is a multifaceted issue, and I'm sure today we don't have time to deal with all of the facets of it. Everything from the issue of personal identification security and protection that has been alluded to the issue of the availability of law enforcement agencies to have access to information for purposes of their investigations, information that in normal circumstances might wish to be secure and protected.

Now all the way to the issue of illegal immigration in our country, with some 7 plus million, many of whom are working in our country and presumably have somebody's Social Security number who don't know and we don't have the knowledge of what the implications of all of that is going to finally be when we sort it all out.

I thank you all for being here today, and I look forward to your testimony, and also to the questions.

Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

The gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. I thank the Chair very much for holding this very important hearing.

Back in the 1960's the Federal Government went to AT&T and asked them if they would be willing to build a packet switch network for the United States. And AT&T said why would we do that, we already have a monopoly. We're not interested in the contract.

And so, they then turned to IBM and asked them to build a national packet switch network, and IBM said why wold we do that? We have a monopoly. We're not interested. And so they turned to a company in Cambridge, BB&N and gave the contract to these very smart scientists at MIT to construct a packet switch network which while providing the role of being a scientific information sharing source of information, also had the additional advantage of providing a redundancy to the existing telecommunications network in the United States. The great fear was that there would be a preemptive attack upon the United States and they would bomb the AT&T national long lines that went right through the middle of the country, decapitating our national leadership.

On September 11 the good news is that this brilliant invention of the scientists at BB&N did work. And even as Verizon or AT&T switches may have been effected, in fact the ability for packet switches to move information and reassemble it regardless of the course that was being taken at the point of destination was something that was really proof positive that the Federal Government in 1967, regardless of what the private sector might have thought about it, really did anticipate September 11.

In addition, I'd just like to note, Mr. Chairman, that we as a committee and I think the Nation as well, has to divide the question. On the one hand we're all very concerned about identifying terrorists within our own country and we're willing to suspend some of the constitutional protections which we would otherwise ensure that everybody, even visitors to our country, were entitled to. And I think all of us, or most of us, at least are willing to suspend that. But we must divide the question between terrorist cells and corporate sellers in terms of the compromise of privacy information. You can't allow any change in attitude in our country to allow corporation America to begin to gain access to information within our country as though anything that happened on September 11 would justify it.

So I look forward to this incredibly impressive panel of experts which you've brought here to us today, lead by our former very distinguished colleague, Mr. McCurdy. And I think it's going to be very helpful to us in understanding what policies should be adopted in the days and months ahead.

Thank you.

Mr. STEARNS. I thank the gentleman.

Ms. McCarthy, would you—are you prepared to——

Ms. MCCARTHY. I'd like to hear from the panel, and I'll put my remarks in the record.

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

And Ms. Harman, do you have an interest in an opening statement?

Ms. HARMAN. Thank you, Mr. Chairman, no. I'd like to hear from the panel.

[Additional statement submitted for the record follows:]

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

Let me begin by thanking the Subcommittee Chair, Mr. Stearns, for calling this hearing on cybersecurity and for assembling such a distinguished panel of witnesses. Let me also thank them, in advance, for their testimony.

Recent events remind us how precious and essential security is—something many of us previously had taken for granted. It is a basic component of our quality of life.

Security also is an essential component of sound and successful commerce—particularly as it relates to the Internet and digital commerce. And I know that recent events have also increased scrutiny—especially by the private sector—of this increasingly important slice of the security umbrella.

The Internet is becoming a larger part of American life and a necessary instrument for American commerce. With more than 60% of Americans with access to the Internet and a great majority of American business interconnected, a certain level of Internet services are on the way to becoming ubiquitous.

The success of Internet services and commerce depends directly on how security is handled by the private sector. For instance, how comfortable and confident consumers and businesses feel with how information is protected, is dependent on the level of security utilized by American business. Unlike national security issues, which are the responsibility of the Federal government, the structure of the Internet—primarily owned and run by the private companies—requires private sector innovation and leadership.

We have seen the huge financial losses suffered by web viruses and worms. We have witnessed the losses by denial of service attacks. Successful cyber attacks can cost companies by disrupting service, exposing them to bad publicity, or manipulating or destroying sensitive company data.

More importantly, successful attacks not only threaten the attacked company and its network but also the company's suppliers, partners, and relationship with its customers. It also effects the non-Internet-driven portion of the company. In essence, attacks create a certain domino effect, which sends economic harm cascading through businesses and Amercans' lives.

In my opinion, the vast majority of American companies are doing a great deal to improve and maintain security in their networks and to ensure the security of information and materials they have.

Even so, there are certain security vulnerabilities in the nature of the Internet and within the networks owned and operated by individual companies. There are some weak points in the inherent architecture. Networks of large American companies will always be targets of criminal attacks, whether by small time hackers or sophisticated terrorists.

However, nobody should take away from this hearing the notion that there is a perilous state in the way companies protect their networks and information. Their ability to create cutting-edge protections against ever-changing threats is simply amazing.

While more work must be done, much work has already been accomplished, just not spoken about—and understandably so. Companies are leery about highlighting how secure their networks are for fear of inviting determined attackers.

I hope that some of today's panelists can speak to the work that their companies are doing to improve the security of their and their clients' networks. I hope they can elaborate a bit on recognition of the relevant issues, assessment testing, deploying necessary resources, and taking corrective measures. Moreover, as security becomes more of a necessity rather than cost-drag on industry, we need to know whether there is a sufficient market developing for solutions and products to improve the Internet security of all companies.

I am also hopeful that this hearing will shed light on what vulnerabilities exist today, what steps are being taken by the private sector to address these vulnerabilities, and what role, if any, the federal government—specifically the Congress—can play to promote increased awareness and action on these issues.

Mr. STEARNS. Okay. All right. We do have, as all the members have pointed out, a full panel and Mr. McCurdy is, of course, a former member. And as sitting members we have great deference and reverence for former members. It's a tandem race. We show deference to them hoping that they'll remember us. But he has the wisdom of both being a Member of Congress and now on the other side. So, we're anxious to hear from him, and we welcome him, personally.

Mr. Doll, I think what we'll do is start from my left and just come across. If each of you would just, in your opening statement, just give us your name and title and then we'll just after your 5 minute, we'll just keep moving down the table.

So I welcome all of you.

STATEMENTS OF MARK W. DOLL, NATIONAL DIRECTOR, SECURITY & TECHNOLOGY SOLUTIONS, ERNEST & YOUNG; DAVE McCURDY, PRESIDENT, ELECTRONIC INDUSTRIES ALLIANCE, EXECUTIVE DIRECTOR, INTERNET SECURITY ALLIANCE; C. WARREN AXELROD, BOARD OF MANAGERS, FS/ISAC LLC; DAVID B. MORROW, MANAGING PRINCIPAL, GLOBAL SECURITY AND PRIVACY CONSULTING PRACTICE, EDS; MARY ANN DAVIDSON, DIRECTOR, SECURITY PRODUCT MANAGEMENT, ORACLE CORPORATION; CHRISTOPHER KLAUS, FOUNDER, INTERNET SECURITY SYSTEMS; JOHN P. CASCIANO, SENIOR VICE PRESIDENT AND GROUP MANAGER SECURE BUSINESS SOLUTIONS GROUP, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION; AND HOWARD A. SCHMIDT, CHIEF SECURITY OFFICER, MICROSOFT CORPORATION

Mr. DOLL. Good afternoon, Mr. Chairman, and members of this committee. And thank you for this opportunity to testify before you today.

I am Mark Doll, National Director of the Security & Technology Solutions for Ernst & Young with over 50 years experience working in cyber terrorism matters.

Ernest & Young is a leading provider of accounting, assurance, and information technology services around the globe, with over 84,000 employees based in 130 countries.

Today I'll discuss the need to assess risk and vulnerabilities of our critical IT infrastructure.

Without being too alarmist, the focus on innovation and the lack of focus on security makes our critical infrastructure vulnerable to attack from criminals, hackers, disgruntled employees and, yes, terrorists. Whether it's via cyber attack, a worm, a virus; any of these things could wreak havoc throughout our interwoven IT reliance chain putting at risk our national security, the way corporate American conducts business and the way civilians and citizens conduct their lives.

So what should we do? Effectively securing our corporate and critical infrastructure systems is no small chore, but we can't be paralyzed by the task at hand. We don't believe that there's any choice but to confront it. Already, however, positive steps are being taken, but more could be done to encourage companies, individuals, the government to address these vulnerabilities and tackle these hard issues.

We need to first address the issues of authentication and authorization, interoperatability, recovery and validation. If we can focus on these concepts, we can take a positive step forward to improving the overall national security. What do I mean by these terms and what do these terms reveal?

First, the term authentication refers to the ability to determine who is using a computer system. And authorization refers to what an authenticated individual is allowed to use or see on a system. Without an appropriate system authentication and authorization, we'll be unable to track and limit unauthorized individuals that might gain access to systems for a personal gain or cyber terrorism.

Second, we need to simplify interoperatability. Interoperatability refers to the ability of systems to function seamlessly, regardless of operating system, application or hardware. Market innovation and competition has driven economic growth and you have tremendous increase in productivity. The same innovation and competition has, understandably, resulted in many proprietary protocols and has created an environment, a very complicated security design which has, in turn, led to security inefficiencies and vulnerabilities. As a result, it is costly and difficult for many organizations to implement truly effective security solutions. Today we must work together in a public/private partnership to simplify these protocols.

Third, recovery. The term refers to the ability to correct system failures and catastrophes in a timely manner. Today, most companies are on their own when it comes to implement fail-safe systems and contingency plans. Many companies lack the necessary rigor and scale of recovery systems to respond to a national attack or cohesive cyber terrorism threat. Any consideration of cyber security must, therefore, take into account a national recovery system.

Finally, validation. Securing our critical infrastructure should not be perceived as a problem that can be fixed simply by purchasing software or installing a firewall. Once a security application or process is put in place, it must be regularly monitored and effectively validated. Unfortunately, there are no common set of standards for validating the security of information systems. Instead, different countries, different individual industries and service providers employ different standards for assessing vulnerabilities and effectiveness of security solutions.

This hampers efforts to conduct comprehensive risk assessments of network safeguards and controls across industries and applications. Service companies like Ernst & Young must then determine how to make these complicated set of standards work within a complex corporate environment while allowing innovation and growth. Any long-term discussion of IT security should, therefore, consider the need to harmonize these standard for validating effectiveness.

In conclusion, critical IT infrastructure security raises difficult issues. Today's hearing is important and is welcome. The President in his Executive Order establishing a Critical Infrastructure Protection Board and the National Infrastructure Advisory Council hold promise. We need to work together in a public/private partnership to answer difficult questions and find effective solutions.

Again, I appreciate the opportunity to outline what we believe will be some of the key issues of this security issue. And I'll be happy to answer questions.

[The prepared statement of Mark W. Doll follows:]

PREPARED STATEMENT OF MARK W. DOLL, NATIONAL DIRECTOR, SECURITY & TECHNOLOGY SOLUTIONS, ERNST & YOUNG

INTRODUCTION

Good morning Mr. Chairman, and thank you for the opportunity to appear before your subcommittee on the topic of security and private sector efforts to address cyber threats. I am Mark Doll, partner and National Director of the Security & Technology Solutions Practice for Ernst & Young LLP. Ernst & Young is a leader in providing accounting, assurance, and information technology services around the globe, with 84,000 employees based in 130 countries.

While the Internet revolution has been occurring, Ernst & Young has been adapting to offer our clients a variety of assurance services aimed at securing their vital information and computer networks. I bring fifteen year's of experience working on IT systems implementations and corporate IT management. Today, my clients include many of the Fortune 500 and new and emerging companies. Of our 84,000 employees, over 1200 work specifically on security and IT risk matters, many of whom come to Ernst & Young from the United States military and intelligence communities. As a result of providing our services to numerous companies, Ernst & Young has a unique perspective on efforts to secure our country's critical IT infrastructure.

Today I will suggest to you that recent events have brought to the forefront longstanding security risks and vulnerabilities throughout our nation's critical Information Technology (IT) infrastructure. In light of this, our nation now needs to work quickly and thoroughly—in public-private partnership—to assess these risks and vulnerabilities and implement effective security policies, not only to address today's problems, but also to prepare for tomorrow's unforeseen challenges.

Security Has Not Kept Pace With Infrastructure Growth and Interdependency

Corporate success has historically depended on the ability of management to control strategic business functions—product quality, management of physical plants, sales, and customer support—to stay ahead of competition. Today, technology has changed the traditional business environment, and is being used to increase productivity and enable the creation of non-traditional business relationships. Competitors are becoming partners, customers can now fulfill their own orders directly from supplier's inventories, and all organizations rely on telecommunications and information systems to manage the day-to-day operations of their businesses.

Yet, as corporate America spent the last decade scrambling to react to and grow at the same pace as its competitors, it gave little regard to the ramifications of that growth. Internet technologies and new business processes created new markets, relationships, and unprecedented access to information systems, but it also created new risks to the security of those networks. Productivity and IT systems grew rapidly; but the security and controls around those systems did not develop at the same pace.

This failure on the part of individual organizations to properly maintain the security of their IT systems could have a potentially disastrous ripple effect on our nation's collective security. Today, every business in America, every citizen who accesses the Internet, creates a portal into our vast interconnected system, creating not only a window through which information is gleaned, but also a potential door through which an attack on the whole system can be launched. Public and private sector organizations rely on many of the same IT systems to maintain productivity. Consumers and businesses today rely not only on their own ability to conduct transactions, but also on the reliability and availability of applications and infrastructure that are managed by others, including their customers, business partners, government, and other companies with whom they have no "traditional" business relationship. This has created a highly interdependent "IT reliance chain" of systems and businesses.

What Is At Risk?

Without being too alarmist, this failure to build security into our systems makes our critical infrastructure vulnerable to cyber attacks not only from terrorists, but also from criminals, hackers, and disgruntled employees. Such individuals often search for the weakest link within a system, sneaking in through a loophole in or between software or hardware systems. Once inside the cyber-perimeter of an IT system, a hacker is then free to disguise him or herself as a valid user, stealing confidential information or creating new vulnerabilities for others to exploit. Whether it is via a cyber attack, a worm, or a deliberately launched virus, a concerted effort could wreak havoc throughout the "IT reliance chain," putting at risk our nation's security, the way corporate America conducts business, and the way citizens live their lives.

Our nation depends on interlinked information systems to run our telecommunications, power, transportation, financial, and national security functions. Business transactions can only take place if the applications and IT systems on which they rely (i.e. software solutions that control manufacturing) are functioning appropriately. But no business is an island of itself. If our nation's critical infrastructure is unavailable, individual businesses will be unable to operate. Similar to a house of cards, if just one component of this chain were to come under attack, the whole network could be affected or, in the worst case scenario, fail.

For individuals, even the most mundane tasks in life are dependent on the proper functioning of the reliance chain. We have become reliant on computer-controlled

systems for banking, telecommunications, power, and also the vital systems that maintain our personal identities, and medical records. An attack on these systems would dramatically affect the American way of life we take for granted, putting at risk our ability to communicate with family and friends, access money, visit a hospital, or even light our homes. We are all highly dependent upon the near 100% availability of our country's critical infrastructure components.

What Needs To Be Done?

The security systems surrounding our critical infrastructure, specifically the information and communications networks, electrical power systems, gas and oil transportation and storage, banking and finance systems, transportation systems, water supply systems, emergency services and government services, must be properly managed.

As you can imagine, effectively securing these systems will be a task of unprecedented proportions. But we must not let the size of the problem paralyze us. Already, hardware and software companies are institutionalizing efforts to proactively post known vulnerabilities and provide patches to their customers. Leading companies are moving quickly to assess vulnerabilities in their operational infrastructures. But we must do more to encourage companies and individuals alike to fix current systems vulnerabilities and tackle head-on the hard issues—such as authentication, authorization, interoperability, recovery, and validation—required for critical infrastructure security.

These are technical terms used by those of us in IT security industry to describe what are actually easy-to-understand concepts. Just as "notice," "choice," "access," and "security" needed to be understood before policy makers could tackle data collection issues, "authentication," "interoperability," "recovery," and "validation" need to be understood and debated if we are to move forward on a national cyber security program.

1. *Authentication & Authorization*—First, "authentication." The term refers to the ability to determine who is using computer systems, how to make sure that individuals are actually who they say they are. "Authorization" is simply what an individual is allowed to use or see on a system. Without an appropriate system for authentication and authorization, we will be unable to track and limit unauthorized individuals that might gain access to systems for personal gain or cyber terrorism.

2. *Interoperability*—The second issue we will need to tackle if we are to ensure security is "interoperability." Interoperability refers to the ability of systems to function seamlessly regardless of operating systems, applications, or hardware. We have today countless numbers of different protocols for operating systems, applications, and hardware. Each vendor has a proprietary interest in their protocols, including the organizations at the witness table with me today. This has created a dysfunctional environment of complicated interoperability between competing systems, applications, and hardware. This limited interoperability makes it costly and difficult for organizations to implement truly effective security solutions.

3. *Recovery*—Third, "recovery." This term refers to the ability to correct systems failures and catastrophes in a timely manner, wherever they occur. Today, we rely on companies to unilaterally act to implement fail-safe systems and contingency plans. Although most have systems to restore a site, network or system failure, it is our experience that many companies lack the necessary rigor and scale of recovery systems to respond to a national attack or cohesive cyber terrorism threat. Any national consideration of IT security must take into account the necessity for a national program requiring and architecting a national recovery system. Admittedly, this will be a costly undertaking on the part of both corporate America and the government.

4. *Validation*—Finally, "validation." Securing our critical infrastructure should not be perceived as a problem that can be fixed simply by purchasing the latest and greatest software or installing a firewall. Once a security application or process is put in place it must be regularly monitored and its effectiveness validated. This applies to all levels of security, including authentication, interoperability, and recovery.

Unfortunately, there is no common set of standards for validating the security of computer and information systems. Instead, different countries, individual industries, application vendors, and hardware providers employ different standards for assessing vulnerabilities and the effectiveness of security solutions. This hampers efforts to conduct comprehensive risk assessments of network safeguards and controls across industries and applications. Services companies like Ernst & Young must then determine how to make all of these competing standards work within a complex corporate environment while allowing for innovation and growth. Any long-

term discussion of IT security should, therefore, consider the need for harmonizing standards for validating effectiveness.

Validation is, in my mind, the most crucial issue we need to tackle, for without it, we will not accomplish systemic change. Only by regularly assessing the effectiveness of controls around complex issues like authentication, interoperability, and recovery will we ensure that any quick fixes are working as intended.

Public Private Partnership Is Necessary

Clearly, critical IT infrastructure security raises difficult issues. Today's hearing is a step in the right direction. We need to work together, in a public-private partnership, to answer these difficult questions and deliberate on effective solutions.

The Administration has issued a call to action to the private sector and government, through the President's October 16th Executive Order creating the Critical Infrastructure Protection Board (the "Board"), to work together to develop standards and best practices necessary to secure information systems for critical infrastructure. Importantly, the Executive Order requires the Board to work with members of the private sector, including the audit community to, among other things, "propose and develop ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems." We look forward to working with the Administration and Congress on this important initiative.

CONCLUSION

In conclusion, the events of September 11, 2001, focused our country's attention on national security issues. It would be a mistake to focus solely on our country's outer security perimeter and overlook the security of our domestic IT infrastructure. We must work together to identify, prioritize and fix known vulnerabilities, as well as identify best practices to ensure the long-term safety and viability of the critical infrastructure on which our economy, citizens, and government rely.

I appreciate the opportunity to be here this afternoon, and am happy to answer any questions.

Mr. STEARNS. I thank the gentleman.

Mr. McCurdy?

STATEMENT OF DAVE McCURDY

Mr. MCCURDY. Thank you, Mr. Chair. Again, thank you for the opportunity to be back on this floor. I lived on this floor for quite a whole, just around the corner. It's good to see my former colleagues.

With your permission, I'd like my statement to be admitted in the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. MCCURDY. And I'd like to just summarize, because having been on that side I know how important it is to get to the bottom line.

There are a number of key points that I'd like to make, and I think this distinguished panel's going to raise a number of very good questions.

Since the chairman alluded to it, I thought I would just give you one graphic. You cited the statistics from the CERT, as did Mr. Doyle. The progression on the security threats, the incidents, each one of these reports is an incident. I Love You was counted as one, the Malissa virus is counted as one. Last year over 22,000 this year at the progression it's currently on, will be over 40,000 separate incidents reported by the CERT.

The important thing with that is the fact that the sophistication of those incidents is also increasing, but the knowledge necessary to perpetrate those attacks and bring back those incidents is actually declining. You no longer have to be a computer genius or, you know, some kind of geek to be able to go in and write software to get into these systems.

A lot of this technology today and the knowledge is on the web. People can collaborate, and you see from a progression those with password guessing now to stealth advanced scanning techniques, automated probes and scans, worms, virus. So this in itself is a disturbing trend.

And I'm going to save the last chart and, perhaps, take it up with a question, and that's the role of government versus the private sector.

I think the threat is real. I think you know that. Many of us has been dealing with this long before September 11. Ms. Harman, knows. She actually sits on the three committees that I sat on; Intelligence, Science and Armed Services, and understands. It's not just a Nation, State, State actor environment. It's a number of individuals and organized crime and other efforts are out there to increase the risk.

There is no such thing, and maybe some of my colleagues might differ, but I don't believe there's such a thing as Internet security or perfect security. If you want perfect security, you can be disconnected from the Internet. You could be totally isolated. But that defeats the purpose of the Internet.

So if you want to be connected, then you're talking about risk management. And there a number of tools and efforts that need to be involved to provide that.

The private sector can do a lot, not just in developing the tools and mechanisms, but improving the standards and best practices, which are management. And Mr. Doll mentioned that, but the important thing there is that this is not a U.S. centric technology. Mr. Markey gave us the Massachusetts' history of packet switching, but this is not a U.S. centric problem. This a borderless technology. It is global in nature, and therefore the risks are global. And it's important that we work on an international basis to provide solutions and reduce this risk.

And the other point that I would make is that, you know, we witness it on a regular basis. Our country, maybe democracies are this way, but we're great at reacting. You know, after September 11 we had incredible forensic evidence and we were able to track these things; the terrorists and their movements and provide a great history. But we're not good in the proactive sense. And I think what we have to do in working with government is develop much more emphasis on developing those practices and standards that prevent and deter, and hopefully preempt some of these attacks. And I believe that the private sector can do that.

The last chart that I was going to mention is one of your charts, not this committee's, but actually the government's. This is actually produced by the CHOW in the Department of Commerce, and it just shows you some of the organization. You saw the other day when Tom Ridge, our former colleague, was sworn in they showed the jurisdictional chart of the 41 agencies that he was involved in. Well, this is for Critical Infrastructure Protection and this chart, too, can kind of drive you crazy.

The public/private partnerships in this are down here in the corner, down here. But I would submit that it's the public/private partnerships in the private sector that's going to do the most to provide the real protection. The government role is simple: Should

take steps and encourage efforts to increase the IT investment, work with CIOs and give them resources to improve the security of the systems of the Federal Government, but then work with the private sector to help establish these best practices and standards and help the industry to see the benefits of further responsibility and accountability at the board level to ensure that there's auditable standards and practices are in place.

And last, Mr. Doyle mentioned Carnegie-Mellon. We are pleased with the establishment of the Internet Security Alliance joint venture with 2300 member companies of EIA and Carnegie-Mellon. It's more than just an FFRDC. In order to expand its reach, to leverage the incredible talent and resources, they need to build their private side of the house in a nonprofit way, which is what ISA's about, in order to get that information and that trusted network of over 40,000 people around the globe who provide over 99 percent of those incident reports. Those aren't generated by the government, those are private citizens around the world that submit those incident reports so that we can gain from that knowledge.

And with that, I appreciate again the opportunity and look forward to our questions.

[The prepared statement of Dave McCurdy follows:]

PREPARED STATEMENT OF DAVE MCCURDY, PRESIDENT, ELECTRONIC INDUSTRIES ALLIANCE, EXECUTIVE DIRECTOR, INTERNET SECURITY ALLIANCE

Chairman Stearns, Ranking Member Towns, and members of the Commerce, Trade and Consumer Protection Subcommittee: I appreciate the opportunity to testify today on behalf of the Internet Security Alliance. I am deeply thankful to Congressmen Stearns and Towns for holding this informative hearing on the private sector's efforts addressing cyber threats.

Since September 11th, the business community has become more security conscious than ever before. There is real alarm among companies concerning not only physical security but also cyber security, and with good reason. According to the CERT/CC at Carnegie Mellon's Software Engineering Institute the number of attacks on the Internet has increased at an exponential rate. The CERT/CC handled over 20,000 incidents in 2000 and are now estimating that they will now handle over 40,000 incidents in 2001. Each one of those "incidents" could ultimately bloom into Code Red or Nimda attack within hours of its detection. The threat is critical. Corporations and the government find themselves on the front lines defending the critical functions of the national infrastructure, as well as the assets of American companies.

In addition, attacks are becoming more destructive, widespread and more difficult to contain. Consider the following information on costs of cyberattacks that businesses have faced recently.

The Cost of Cyberattacks

- SirCam: 2.3 million computers affected
  - Clean-up: $460 million
  - Lost productivity: $757 million
- Code Red: 1 million computers affected
  - Clean-up: $1.1 billion
  - Lost productivity: $1.5 billion
- Love Bug: 50 variants, 40 million computers affected
  - $8.7 billion for clean-up and lost productivity
- Nimda
  - Cost still to be determined

In April of 2001, Carnegie Mellon University and the Electronics Industries Alliance formed the non-profit *Internet Security Alliance* to advance the efforts of the private sector in the information security debate. You may know that the majority of the Internet, over 80%, is owned and operated by the private sector. Private sector leadership is essential to determining an overall strategy to increase the strength and survivability of the Internet. The Internet Security Alliance seeks to help in this endeavor

As the Internet continues to ingrain itself as a linchpin of American business and with concern growing that the cyber environment is ripe for attack, industry now more than ever needs an independent, non-partisan organization that offers comprehensive, universal threat sharing and assessment, and collaborative solution development. We need to create a new paradigm for global information sharing to help companies that rely on the Internet deal with the growing threats to their continued success and growth.

Furthermore, since 80 percent of technical vulnerabilities are common to all organizations, and misperceptions about robust security can lead even the most attentive security engineers to expose their systems to attack. Industry needs to develop universally recognized information security practices capable of being pushed down through supply chains so evolving Internet threats can be effectively mitigated and deterred. You are only as secure as your weakest link.

The Internet Security Alliance is one of the few organizations working on behalf of industry to address these issues. With its international and multi-industry segment member representation and access to a network of more that 40,000 loyal systems administrators and security engineers who diligently report new threats and vulnerabilities, the Internet Security Alliance is redefining the concept of information sharing. On a near real-time, systematic basis, the alliance provides companies large and small with access to trusted and reliable information, solutions and decision support tools to help mitigate the vulnerabilities and emerging threats we are here to discuss today.

Driven by some of the brightest security minds in industry and academia, the alliance has also begun work on a robust set of best practices that will serve as guiding principles for companies and their supply chains as they evolve their security policies and procedures. Our efforts enable companies to allocate their limited resources on other projects, such as deploying intrusion detection systems, firewalls, and raising security awareness within their company.

Using the collective experience the Internet Security Alliance and its members, we can effectively promote sound information security practices, policies and technologies that enhance the security of the Internet and global information systems.

Why is the private sector involvement so important?

The Internet Security Alliance applauds the efforts of the current Administration in its dedication to raising the awareness of cyber-threats and cyber-terrorism. It's leadership on the recent cyber-attacks on Code Red and Nimda were invaluable to testing the true value of both private and public partnerships. On the government side, officials tend to view private sector participation as well as the agency involvement in terms of sectors or "stovepipes" (see attached chart for the government organization chart for cyber-security), therefore creating barriers to true information sharing. The private sector is critical of this approach and is looking for more inclusive participation from all sectors. In order to maximize the effectiveness of taking on the cyber-security issue, collaborations and communications should be cross-sector and horizontal to all companies and government entities (where appropriate). We are all facing a common threat with respect to cyber-terrorism and vulnerabilities and will need to work together in order to protect our most critical assets.

International problem vs. U.S. centric problem: Cyber-Security

The Internet knows no boundaries and is accessible from most parts of the world. As the Internet continues to be a tool that promotes the openness of ours and many other societies, it brings along vast risks and vulnerabilities. The Internet operates with no bias or cultural differences—it provides information and interaction. Since the concept of the Internet was based on the issue of trust, we can see the probability of its being compromised fairly easily.

With that in mind, we would be foolhardy to not communicate with other nations on their experiences and potential remedies for cyber-attacks that have happened on their networks. Not taking into account the expertise of foreign security experts would put the U.S. effort at a severe disadvantage. In addition, if the U.S. is not inclusive of other countries in this global problem, we stand to weaken our resolve to protecting ourselves by operating with limited knowledge of potential threats.

Proactive Measures vs. Reactive Response

Finding solutions to cyber-security vulnerabilities and attacks has been historically reactive. Attacks happen, analyses made and a patch would be provided, if possible. We cannot continue to solve individual attacks on a case-by-case basis, while not addressing the larger problem. A better approach is to implement practices and policies that improve the protection of our networks by thwarting a higher percent-

age of attacks. In other words . . . becoming more *proactive* in our approach to cyber-security. By promoting practices currently in place for more security-focused companies and tailoring them for other sectors, additional protection could be provided. Many companies, especially medium-sized and smaller firms are vulnerable and looking for assistance in determining what security practices can help them better protect their systems.

Private and Public Partnerships

The security and survivability of the Internet depends on the cooperation between the private and public sectors. Congress should promote interaction between government and the private sector and should also address issues such as exemption from FOIA and anti-trust barriers. In addition, Congress can set a great example for the private sector by increasing the security of all government systems, which historically have been out-dated and have not met minimal standards for security.

The Internet Security Alliance is able to act as a bridge between the private sector and public sector by promoting best practices and appropriate data sharing mechanisms. The Internet Security Alliance is also involved in the following activities:

- Providing thought leadership on information security issues
- Representing industry's interest on information security issues before legislators and regulators
- Creating mechanisms that cause rapid development and implementation of information security practices, policies and technologies
- Identifying and standardizing best practices in Internet security and network survivability
- Creating a collaborative environment to develop and implement information security solutions
- Promoting universal sharing of information and intelligence on emerging threats/ vulnerabilities/ countermeasures
- Information Sharing
  - —Providing vulnerability catalog, threat alerts and analysis, executive communications, call center, trend briefings, economic impact analysis
  - —Shaping and influence practices and resources at CERT/CC to meet the needs of industry
- Best Practices/Standards
  - —Establishing common benchmarks
  - —Evaluating relevance of existing standards, define gaps and agree on relevant and uniform criteria for standards moving forward
  - —Developing a Software Seal of Approval
- Policy Development
  - —Providing decisive influence on the public policy issues whether nationally or internationally
  - —Targeting cybercrime and terrorism, privacy, information sharing, corporate responsibility and leadership on information security issues
- Security Tools
  - —Sector-tailored versions of OCTAVE®
  - —Sharing of R&D expertise of Alliance members

To summarize, only by combining the strengths of both the private sector and public sector on issues such as early warning detection and information dispersal, promotion of best practices, agreement over sound information security policies will we be able to turn the tide on the cyber-security threat facing our nation.

The Internet Security Alliance is poised to represent and promote the needs and views of the private sector on cyber-security. We thank the committee for its interest and for allowing us to participate in this necessary and timely hearing.

Mr. STEARNS. I thank my colleague.

Mr. Axelrod?

STATEMENT OF C. WARREN AXELROD

Mr. AXELROD. Thank you, Chairman Stearns, and members of your subcommittee for the opportunity to address you today on the very timely questions of what the private sector is doing to protect itself against cyber attacks, what it should be doing and how government might help.

I would also ask for my written statement to be included in the record.

My name is Warren Axelrod, I'm a Director responsible for global information security with the Pershing Division of Donaldson, Lufkin and Jenrette Securities Corporation, which is a Credit Suisse First Boston company.

I'm also on the board of managers of the Financial Services Information Sharing and Analysis Center for the FS/ISAC.

Today I will share with you my thoughts and suggestions on cyber security as someone who is an information security professional and a practitioner with more than a quarter of a century's experience as an information technology manager in the financial services industry.

It's well known that with the relatively recent and rapid adoption of the commercial Internet, government and business have become increasingly dependent on a critical infrastructure over which they have little or no control. Largely due to this lack of control, we have see a proliferation of damaging computer viruses, worms, denial-of-service attacks and network and system breaches. With such an accelerating use of the Internet, the impact on commerce of unintentional network and deliberate acts of terrorism and compromise is greater each day.

While thousands of new viruses and worms are created each month, relatively few cause significant damage. However, millions of scans of the Internet run each day by those seeking out weaknesses, only a very small percentage actually result in compromises. However, since the number of attempted attacks and the population of potential victims are both so enormous, even a very small rate of success has produced estimated damage in the billions of dollars per year.

Since at this time deterrence is not sufficiently effectively and the pressure is on to expand services over the Internet, we are left with preventative measures as our best hope for reducing potential damage from cyber attacks. The greatest counterforce in this battle is, in my opinion, information sharing. Knowledge of new threats, newly discovered weaknesses and actual incidents gives organizations the opportunity to prepare for impending attacks or prevent exploitation by closing off known vulnerabilities. This is where the FS/ISAC comes in.

The FS/ISAC is an industry funded product of Presidential decision directive 63 on critical infrastructure protection. PDD 63 required government agencies to partner with the sectors that make up critical infrastructure. The PDD additionally suggested that all critical sectors from ISAC to collect and analyze threat vulnerability and incident data.

The U.S. Department of the Treasury is the partner of the banking and finance sector, and has been extremely supportive of the FS/ISAC.

A key feature of the FS/ISAC is it allows members to submit information anonymously while insuring that submittals are from an authentic source.

More recently, the banking and finance sector has ramped up several initiatives, including a crises management committee initiated by the Banking Industry Technology Secretariat and the Busi-

ness Continuity Committee established by the Securities Industry Association.

While I believe that the banking and finance sector has reason to be proud of initiatives that it has already put in place, there remains a considerable amount still to be done before we can feel comfortable with our state of preparedness.

There are many ways in which Congress can help promote programs and processes to improve our defenses against cyber attacks and our ability to handle them. The willingness of industry members to share information, particularly about cyber incidents with other members of the ISAC would be much greater were there not the fear of infringing anti-trust laws.

The ability of private industry to share security information with government depends very much on obtaining an exemption from the Freedom of Information Act, which would eliminate concern that damaging information would become available to competitors and potential attackers.

Both of these items are central to the Critical Infrastructure Information Security Act of 2001 proposed by Senators Bennett and Kyl for which there has not yet been any inclusion in the legislative calendar. The proposal in the Act are key if we are to encourage a much broader sharing of important security related information.

I would like to suggest to Congress that it revisits this issue and, if possible, accelerates litigation such as the Bennett Kyl bill. Similar legislation worked for year 2000 and it can work against cyber terrorism as well.

We need the ability to pursue cyber attacks and prosecute them fully if we are to discourage others from attacking out networks and computers. I would propose that Congress consider legislation to further empower law enforcement to track down perpetrators.

We also need reciprocal arrangements with friendly countries so that they will support these endeavors.

I believe that the government should support the establishment of separate secured private Internets such as the proposed government network. I suggest that Congress encourage the development of these networks by providing appropriate and if necessary, authorizing funds to seed them.

I would propose that Congress consider supporting programs to educate our people about the importance of maintaining the security of the networks and computers of our critical infrastructure.

I would suggest that Congress consider funding a permanent information coordination center along the lines of that established for the year 2000 period, which was subsequentially dismantled. There should be a dedicated section in the center for cyber security.

Finally, I would suggest that Congress support the development of a national strategy for protecting the Nation's critical infrastructure.

I recognize that I am proposing a costly series of programs at a time when budgets are tight. However, the size of threats are very real and we must protect ourselves against them. It will be a long and bitter battle, but we must engage in it if we are to prevail.

Mr. Chairman, again, thank you for the opportunity to present to you and your subcommittee.

This concludes my statement. I will be happy to answer questions.

[The prepared statement of C. Warren Axelrod follows:]

PREPARED STATEMENT OF C. WARREN AXELROD, BOARD OF MANAGERS, FS/ISAC LLC

I wish to thank you, Chairman Stearns, and the members of your Subcommittee on Commerce, Trade and Consumer Protection, for the opportunity to address you today on the very timely questions of what the private sector is doing to protect itself against cyber attacks, what it should be doing, and how government might help the private sector in accomplishing its goals.

Mr. Chairman, you and your subcommittee members, show both foresight and insight in focussing your attention on protecting our critical infrastructure from cyber attacks against the computer systems and networks upon which the economy of the United States of America increasingly depends. You are to be commended for tackling this important category of risk to commerce at a time when the Nation is distracted by the tragic events of September 11th, an unresolved bioterrorism attack, and a war in Afghanistan.

Just one week after the September 11th terrorist attacks, our computer systems and networks were hit with one of the most devious and sophisticated cyber infections to date—the Nimda worm. Nimda is an example of a new generation of malicious software, or malware, that spreads in many ways and is difficult to eliminate from infected machines.

Perhaps the Nation's initial focus on the aftermath of the physical attacks, followed a short time later with a frightening anthrax scare, made Nimda appear less of a threat than it actually was. The impact of Nimda was also considerably mitigated by organizations having patched their systems as a result of the Code Red worm, thereby providing greater protection. However, many security professionals see this evolution in cyber-attack capability as a very disturbing and ominous trend. The timing of the Nimda attack is also noteworthy, since it was launched at a time when a number of major financial organizations were operating in less-than-ideal disaster recovery modes. This suggests the recognition by cyber attackers that their activities can be even more effective against targets that are already weakened.

MY PERSPECTIVE

I am a director, responsible for Global Information Security, of the Pershing Division of Donaldson, Lufkin and Jenrette Securities Corporation, a Credit Suisse First Boston company.

Today, I intend to share with you my thoughts and suggestions on cyber security as someone who is an information security professional and a practitioner with more than a quarter of a century's experience as an information technology manager in the financial services industry.

It is a great honor for me to represent the securities industry and I hope that my testimony will lead to measures that will help in some ways to protect our Homeland from the costly effects of cyber attacks. I wish to thank the SIA (Securities Industry Association) for their support in preparing for this hearing.

As one of the founders of the FS/ISAC (Financial Services Information Sharing and Analysis Center) and a current member of its Board of Managers, I am firmly committed to the important role of information sharing in assisting the financial services industry in protecting itself from malicious cyber attacks.

In the late 1990s, I co-chaired two SIA committees on Year 2000 contingency planning and event management, which provided extensive guidance for the financial services industry. I recently recounted those efforts to the industry to help deal with today's heightened fears, which are not much different from those preceding Year 2000.

Over the millennium weekend, I served in the Cyber-Assurance National Information Center, representing the banking and finance sector. The Cyber NIC was located adjacent to, and continuously in contact with, the Information Coordination Center(a center established by the Federal government to coordinate across state and local governments as well as with industry sectors. I was with a group of private sector volunteers who were monitoring the condition of cyberspace during a time of great concern over potential cyber attacks. That apprehension was not unfounded.

THE NATURE OF CYBER THREATS

It is well known that, with their relatively recent and rapid adoption of the commercial Internet, government and business organizations have become increasingly

dependent on a component of the critical infrastructure over which they have little or no control. Largely due to this lack of control, we have seen a proliferation of a whole variety of damaging creations and activities, such as viruses, worms, denial-of-service attacks and network and system breaches. With such accelerating use of the Internet, the impact on commerce of unintentional network and system breakdowns and deliberate acts of destruction and compromise is greater each day.

Another way in which cyber malfeasance differs from physical acts of terrorism, is that location, cost, and fear of arrest and punishment do not seem to hinder or deter cyber terrorists. While thousands of new viruses and worms are created each month, relatively few make it from "the zoo" into "the wild" and cause significant damage. While there are millions of scans of the Internet run each day by those seeking out weaknesses, only a very small percentage result in actual system compromises. However, since the number of attempted attacks and the population of potential victims are both so enormous, even a very small rate of success has produced estimated damage in the billions of dollars per year over the past several years.

Some forms of malware, such as viruses, are released onto the Internet by their creators and spread from system to system through the unknowing complicity of others, not unlike their physical counterparts. Modern viruses and worms frequently incorporate "social engineering" to get their unwitting accomplices to take actions, such as opening an e-mail attachment, that will propagate their payloads. The "I LOVE YOU" virus was a crowning example.

Terrorist groups or hostile countries would not generally use viruses and worms to compromise an enemy's computer systems and clog its networks, since such attacks are not directed and could just as easily impact friends as enemies. Rather they would target specific Web sites or computer systems.

We have seen that virus developers and activators (who are not necessarily the same individuals) tend to be out to undermine society in general or make a name for themselves among their peers. However, the damage from viruses to commerce and government can be very large, and measures are needed to reduce their impact, if not eliminate them entirely.

Cyber attacks that are more directed can take several forms. Most commonly, the attacker will search for exposures in the software products and equipment that typically make up organizations' defenses and seek access into such systems by exploiting their vulnerabilities. When access has been gained, the attacker will try to gain control of the system as a so-called privileged user. Once in control, the attacker may destroy, alter or steal data (including nonpublic, personal consumer information), programs and other information assets, such as credit card numbers, or may change various features of the system, such as by defacing public Web pages. Alternatively, attackers may leave some program code in place to facilitate their own future access and potentially perpetrate a distributed denial-of-service attack on a particular Web site.[1] The targets of such attacks are determined in advance, and the attackers have to take specific actions (versus their passive role in the spreading of computer viruses) to carry out such an attack.

It is because cyber attacks can be hugely disruptive and costly that we are compelled to take protective measures.

MEASURES THAT HAVE BEEN TAKEN

In this section, I will discuss what measures have been taken generally, and, where appropriate, by the banking and finance sector in particular, according to the categories of deterrence, avoidance, prevention, recovery and restoration.

Deterrence

From an economic perspective, it does not really matter what the source or type of attack may be. After all, the damage can be much the same from a virus, worm, denial of service, or information destruction or theft, whether the perpetrator is a recreational hacker, terrorist, or hostile government or government-sponsored group. Indeed, internal staffs have initiated some of these same compromises, whether intentionally or not.

However, from a deterrence point of view, there is a big difference. If the source is domestic, then there is a greater possibility of arrest and due process, whereas if the attacker is in a foreign country, particularly one hostile to the U.S., the chances of capture are much diminished, even when the perpetrator is identified.

---

[1] In a distributed denial-of-service attack, the attacker will compromise a number, perhaps in the hundreds or thousands, of weakly-defended computer systems and turn them into "zombies" by depositing some program code on those systems. At a particular point in time, the attacker will instruct all the zombies to direct a flood of messages at a specific site, which is overwhelmed and taken out of service.

Law enforcement has tracked down quite a number of violators, but in general the risk of apprehension has been low and the punishment moderate. I think that we can safely say that deterrence generally has minimal effect and that the attacker population continues to increase rapidly, as can be seen from the continuing upward trend in the number of incidents and the increasing effectiveness of their weapons (i.e., viruses, worms, and other malicious programs).

Avoidance

The ease of use, global reach and low cost of the Internet have been major motivators for government and business, as well as for individuals, to move commercial activities to the Internet. With this growth, however, comes the increasing risk of cyber attacks. Even if it were desirable, which it generally is not, restricting the use of the Internet is difficult to accomplish, although many have stated that electronic commerce (e-commerce) has been significantly held back due to the lack of security, and hence privacy, for commercial transactions.

In such situations implementing security measures is seen as enabling commerce in situations where consumers' information would not be protected adequately without the measures. Thus, it is possible to have a Web site certified by a third party. However, many customers are not aware of these certifications nor is there overwhelming evidence that customers choose one site over another because of certification.

Many organizations use specialized software products to block employees' access to certain Web sites that they deem inappropriate. This tends to reduce the risk of accessing less well-protected Web sites that might be harboring a worm, such as Nimda. Similarly, organizations strip off specific attachments on incoming e-mail, such as those with file names with "exe" extensions, which are more likely to harbor viruses and worms.

There are signs that private Internets may be considered an answer to cyber security in some situations, as with the recent call for a private GovNet by Richard Clarke, recently-appointed chairman of the President's Critical Infrastructure Protection Board.

Avoidance served to reduce risk considerably during the Y2K date transition period. Over that weekend, in particular, many companies shut down their Internet connections, and took their computer systems off line. There were also fewer aircraft in the air and many, who would normally be out celebrating such an occasion, were at work monitoring their organizations' computer systems and networks. While difficult to quantify, such tactics may well have resulted in far fewer incidents than might have been expected.

Prevention

Since, at this time, deterrence is not sufficiently effective, and the pressure has been to expand services over the Internet rather than restrict them, we are left with preventative measures as our best hope for reducing potential damage from cyber attacks. The principle behind prevention is to identify and block cyber attacks as they happen using technologies such as routers, firewalls and intrusion detection software. E-mail is scanned for pre-specified words and phrases and those items that appear suspicious are quarantined. Commercial software is "patched" with the latest "fixes" to eliminate known vulnerabilities, which might otherwise be exploited directly by a hacker or through a virus or worm or similar piece of self-generating malicious software.

If the world of cyber threats were static, then the above measures would eventually eliminate risks due to those threats. However, that is not the case. As mentioned above, there is a constant torrent of new dangers, and the government and business worlds must struggle to keep up with them. The greatest counter-force in this battle is, in my opinion, information sharing. Knowledge of new threats, newly-discovered weaknesses, and actual incidents that have happened to others in their industries and elsewhere, gives organizations the opportunity to prepare for impending attacks or prevent exploitation by closing off known vulnerabilities. This is where the FS/ISAC comes in.

The FS/ISAC

The FS/ISAC was a product of Presidential Decision Directive Number 63 (PDD 63) on Critical Infrastructure Protection, dated May 1998. PDD 63, which incorporated President Clinton's critical infrastructure strategy, required government agencies to partner with the sectors that make up the critical infrastructure. The PDD additionally suggested that various industry sectors form Information Sharing and Analysis Centers, or ISACs, which would collect and analyze threat, vulnerability, and incident data. The U.S. Department of the Treasury is the designated partner of the banking and finance sector. Treasury has been, and remains, ex-

tremely supportive of the FS/ISAC. Treasury Secretary Robert Rubin was very encouraging during the initial stages of the critical infrastructure effort for the banking and finance sector and Treasury Secretary Lawrence Summers officially launched the FS/ISAC on October 1, 1999.

With almost 50 full-time members and another 50 firms in a trial program, the member companies of the FS/ISAC membership account for the processing and protection of perhaps 80 percent of the financial assets handled by U.S. financial institutions. The FS/ISAC provides warnings of threats and vulnerabilities, up-to-the-minute notification of incidents as they unfold, and helpful advice as to how to avoid or prevent threats from turning into disasters. It does so according to a unique model, which I will now describe.

The FS/ISAC derives its information from many sources, including government agencies. Members are expected to report security information or experiences to which they are privy. This information can be submitted anonymously or can be attributed, at the member's discretion. While, for anonymous submissions, the FS/ISAC does not know the originator of the information, authentication technologies ensure that the submitter is actually with a member company.

The FS/ISAC analyzes incoming information with respect to validity, importance, timeliness, and severity. If the submission passes muster, it is then "scrubbed" to remove all indications of the source (unless it is expressly permitted to reveal the source), and notifications, with warnings as to their urgency, are disseminated to members via e-mail, pager, telephone or fax. Unfortunately, over the past two months, members have received distressingly many alerts marked crisis or urgent.

Redundancy, Recovery and Repair

Despite best efforts, it is not always possible to prevent cyber threats from succeeding, so that a number of incidents of varying severity do occur.

In most cases, security compromises or breaches can be quickly resolved through the use of alternative on-site networks and systems, while the compromised systems are being repaired. For this to be possible, suitable redundant facilities need to be planned and installed in advance.

If a cyber attack renders a site unusable, an organization must turn to its business continuity and/or disaster recovery plans as well as its crisis management capabilities in order to operate in recovery mode at a different location. It should be noted that a location can be rendered unusable if, for example, a cyber attack were to take down other parts of the critical infrastructure, such as the electrical power grid or telecommunications network.

In financial services, many companies had developed contingency plans for Y2K. It was reported that a number of firms located in and around the World Trade Center invoked their Y2K plans in response to the events of September 11th and that the devastating impact of the catastrophe on firms was considerably less because they were better prepared. Since then, the banking and finance sector has ramped up several initiatives, including a crisis management committee initiated by BITS (Banking Industry Technology Secretariat) and the Business Continuity Committee established by the SIA. As mentioned previously, the SIA had played an important leadership role in Y2K contingency planning and established a command center in New York, with which I was able to communicate from Washington over the Y2K weekend.

The financial services industry, in particular, has developed extensive contingency plans, due to the criticality of their operations to the economy and from having to meet strong legislative and regulatory requirements.

WHAT STILL NEEDS TO BE DONE

While I believe that the banking and finance sector has reason to be proud of the initiatives that it has already put in place, there remains a considerable amount still to be done before we can feel comfortable with our state of preparedness.

Information Sharing

The FS/ISAC model for the sharing of cyber security information has been adopted by a number of other critical sectors at home and by several countries internationally. In addition, the FS/ISAC has had discussions with these and other ISACs regarding the sharing of cyber security information, while still maintaining anonymity of the source when desired. The goal is to have a global network of "friendly" ISACs to leverage the advantages of a broader reach and a larger population of incidents from which to derive patterns of activities that might lead to an attack.

The FS/ISAC receives information from many government agencies, including intelligence and law enforcement, and disseminates it among its members. Unfortu-

nately, it is not yet feasible to return the favor and provide government with information that the FS/ISAC has obtained from its membership, since there are antitrust and freedom-of-information issues that need to be resolved.

I feel strongly that the broadcasting over the Internet of information about vulnerabilities by those who think that they are benefiting mankind by forcing software vendors to strengthen their products is misguided and damaging to the information infrastructure. For example, the Code Red virus appeared just a couple of weeks after a security expert had posted a notice on the Internet about a specific vulnerability in a particular piece of Web server software for all to see. His rationale was that the particular software vendor had not responded to his exhortations to fix the problem. Code Red resulted in possibly billions of dollars in lost business. How much better would it have been if the network of ISACs had been informed and had distributed the information on a need-to-know basis to its members? In fact, members of the FS/ISAC had received prior notice of an update to the software in question that, if applied to their systems, avoids the effects of this particular virus.

Outreach, Education and Training

There is a clear need for reaching out to the general public, educating them about cyber security and making them aware of reasonable precautions that they might take to limit the impact of a cyber attack. This should be done without arousing undue concern or revealing information that would not be in the national interest.

There is a severe shortage of qualified information security professionals to handle the broad spectrum of knowledge and capabilities required in order to protect our government agencies and private businesses from the increasing threats to the computers and networks that make up the critical infrastructure. We need programs to educate and train the requisite numbers of individuals in the basics if information security and to provide on-the-job training for practitioners in related areas. Some private companies are already doing this, but security certifications of various types need to be encouraged so that more of those on the Internet have taken necessary actions to secure their system and network environments.

A National Strategy

It is key to educate the general public and those in leadership positions of the issues surrounding cyber security and its importance of sustaining the critical infrastructure. Several National Plans for ensuring the protection of the U.S. critical infrastructure systems have been written. One for government agencies was published in January 2000. Sector plans have been developed but not disseminated as yet. I worked on the draft of the Banking and Finance Sector National Plan for Information System Protection. These planning documents, or ones very like them, should be shared with industry leaders and the public and should become the basis for a National Strategy for Homeland Security, as it relates to cyberspace.

At the moment the destiny of the National Plan documents is not clear. Prior to the establishment of the Office of Homeland Security, the Critical Infrastructure Assurance Office (CIAO) was coordinating the collection and aggregation of the plans from the various critical sectors.

Research and Development

One way to keep up with, and even get ahead of, cyber attackers is to develop tools with the ability to rapidly identify and block attacks, to determine vulnerabilities in deployed systems and networks, and to discern suspicious activities before they develop into full-blown attacks. An active, well-supported research and development program for cyber security should be initiated. The topics being researched need to have a strong practical bent and meet the needs of the private sector.

Separate Networks

The building of separate, restricted and highly secured networks, using the technology of the Internet but not being as accessible to everyone, is something to consider in the light of the risks in using a public, uncontrolled network environment. GovNet might be the first, but others should follow as the concept proves itself.

Simulation Modeling

As the complexities of modern economies become even greater, it is not possible for an individual, or group of individuals, to understand all the complicated interactions and dependencies of the various components on one another. This can only reasonably be achieved through the use of simulation models to express the interdependencies and provide the capability to examine what might happen if certain parts of the infrastructure were to fail or be brought down by a cyber attack.

Contingency Planning, Incident Response and Crisis Management

As mentioned above, the initial steps have been taken in the banking and finance sector to reconstitute the information coordination centers of the Y2K era, with their attendant contact lists, chains of command, and information gathering, analysis and reporting systems. Once communication, coordination, command and control capabilities have been established, it is important that they are maintained at some level on a round-the-clock basis into the foreseeable future and can be ramped up rapidly to full-scale operations when an incident occurs.

RECOMMENDATIONS FOR CONGRESSIONAL ACTION

There are many ways in which Congress can help promote programs and processes to improve our defenses against cyber attacks and our ability to handle them.

Information Sharing

The willingness of industry members to share information, particularly about incidents, with others members of an ISAC would be much greater were there not the fear of infringing antitrust laws. The ability of private industry to share security information with government agencies depends very much on obtaining an exemption, for this type of information, from the Freedom of Information Act, since that would eliminate the concern that damaging information would become available to the public, including competitors and potential attackers.

Both of these items were central to the "Critical Infrastructure Information Security Act of 2001" proposed by Senators Bennett and Kyl, but which has not yet been included in the legislative agenda. The proposals in the Act are key if we are to encourage a much broader sharing of important security-related information. This would to lead to broader availability of much more valuable information and strengthen our ability to protect ourselves from cyber attacks.

I would like to suggest to Congress that it revisits this issue and, if possible, accelerates legislation such as the Bennett-Kyl Bill. Similar legislation worked for Year 2000, and it can work against cyber terrorism as well.

Deterrence

We need the ability to pursue cyber attackers and prosecute them fully, if we are to discourage others from attacking our networks and computers. I would propose that Congress considers legislation that will further empower law enforcement agencies to track down perpetrators of cyber crime. In addition, we need reciprocal arrangements with friendly foreign countries so that they will support and participate in these endeavors.

On a global level, it may be reasonable to expect a commitment of funds for law enforcement to counter cyber terrorism among the more prosperous and advanced countries of the industrial world. However, this may not be true of so-called Third World countries, especially those from which attacks emanate. Cyber terrorism coming from hostile countries requires special consideration and response.

Avoidance

I believe that the government should support, and subsidize where appropriate, the establishment of separate secured private Internets, such as the proposed GovNet network. I suggest that Congress encourage the development of these networks by providing appropriate support and, if necessary, authorizing funds to seed these initiatives.

Outreach, Education and Awareness

I would propose that Congress consider supporting programs to educate our population about the importance of maintaining the security of the networks and computers that constitute much of our critical infrastructure. Also, I suggest that the government should consider special programs, such as subsidizing college-level studies, to develop information security professionals.

Research and Development

While I am very much in favor of promoting research and development programs to come up with ideas and capabilities to improve our cyber security, I am concerned that such research might not result in a sufficient number of practical solutions. I suggest, therefore, that R&D programs be conducted with some industry representation so that the results meet the needs of real-world entities.

This is an area for which the best use of funds is not obvious. Therefore I suggest to Congress that a study be conducted, in conjunction with the private sector, to ascertain the best way to generate new ideas in cyber protection.

Simulation Modeling

The development of simulation models that appropriately represent the critical sectors, their mutual interactions, and the impact of component failures is a daunting task. I am aware that Los Alamos National Laboratories and Sandia National Laboratories have done work in this area. I would recommend that Congress should support and encourage these efforts but that, before major commitments are made, the requirements of the models be determined by a working group that includes subject-matter experts from various critical sectors. Industry and government representatives should participate in the design process to ensure that the models are realistic and useful.

Contingency Planning and Event Management

I would suggest to Congress that it should consider approving funding of a permanent Information Coordination Center (ICC) along the lines of the one which was established for the Year 2000 period, and which was subsequently dismantled. A mix of individuals representing both government and the private sector should staff the ICC. Under normal conditions, the ICC would have a minimal level of staffing, but have the capacity to rapidly grow to full capability if an emergency is declared.

I believe that there should be a dedicated permanent section of the ICC that focuses on cyber security, rather than the ancillary arrangement that existed during Year 2000. The cyber security group requires extensive and immediate access to top experts in the field as well as an advanced capability to continuously monitor activity on the Internet.

National Strategy

Finally, I would suggest to Congress that it should support the development of a National Strategy for protecting the Nation's critical infrastructure and that participants from the various sectors be included in the development of the plans in conjunction with representatives from assigned government agencies.

CONCLUSION

I recognize that I am proposing an extensive and costly series of programs to protect the Nation's critical infrastructure from increasingly dangerous and damaging cyber attacks, especially during a time of diminishing budgets. The cyber threats are very real, as we have seen in recent years, and we must protect ourselves against them. It will surely be a long and bitter battle, but we must engage in it if we are to prevail, which we must. Unfortunately, the impact of a very successful cyber attack can far exceed that of many of the physical attacks, which we have seen in recent weeks and about which we speculate.

Mr. Chairman, I want to thank you again for the opportunity to present my thoughts and experiences to you and your Subcommittee. This concludes my prepared statement. I am happy to answer any questions that you and other members of the Subcommittee wish to ask.

Mr. STEARNS. And I thank you.

Mr. Morrow. Just pull that mike right close to you.

STATEMENT OF DAVID MORROW

Mr. MORROW. Thank you, Mr. Chairman.

Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify before you today.

My name is Dave Morrow, and I'm the Managing Principal for the Global Security and Privacy Consulting Practice of EDS. I have over 25 years of experience in the information technology field as a computer crime investigator, an IT security officer and an IT manager.

I'm honored of this invitation to present to this subcommittee on EDS' views of the state of information technology security in U.S. industry.

I will submit my full testimony for the record and summarize for you now.

The tragic events of September 11 have brought many changes to our way of life. One of the changes are the physical security of

public places such as airports and sports venues. We have witnessed a dramatic increase in the attention being paid to the security of what our Chairman and CEO Dick Brown has referred to as today's economic currency; knowledge and information.

Over the past several years the frequency and severity of cyber attacks against both government and commercial infrastructures has increased dramatically. While many if not most of these attacks are relatively minor, such as website defacement and simply harassment, others are designed to cripple, damage or destroy the computer networks they encounter.

For example, our own EDS network infrastructure detects and neutralizes over 20,000 viruses, worms and network attacks per month.

Our economic system is based on trust; trust between trading and investing partners, trust between consumers and merchants, trust between suppliers and purchasers. If this sense of trust is damaged or destroyed, our economy would be crippled. Maintaining these trust relationships is one of the most important things we all can do to ensure the continued development and growth of our information economy.

Since September 11, however, we have seen a great interest in expression of concern from corporate management and request for information from our clients about IT security. We've doubled those requests, especially in the areas of business continuity planning and overall security best practices.

Tragic is a word and the events of September 11 have helped drive home the fact that security should be considered an essential investment rather than simply an expense to be minimized. Overall, however, I would characterize the state of IT security industry as poor and struggling to improve. While many Fortune 500 corporations focus a good deal of attention to security, many small and medium organizations, both in and out of government, still leave the bulk of the work of securing their systems to individuals who perform these critical tasks as an addition to their normal jobs and have little training to do so. According to the Federal computer incident response center, about 90 percent of successful attacks are caused by the lack of updated software patches, a task that is a basic to good security practice.

A striking example of this can be found in the fact that the Code Red worm, which wreaked havoc on numerous corporate systems a few months ago, took advantage of computer vulnerabilities that had been identified and corrected by a software patch months before.

Finally, while we have seen a laudable increase in spending on many aspects of physical security since 11 September, there appears to be little increase in funds allocated to strengthening the security of the commercial information infrastructure which fuels our economy.

So what can be done? First, we can concentrate on developing a more coordinated program of industry/government cooperation that stretches beyond the critical infrastructures designated by PDD 63 to encompass a wider variety of companies and institutions.

Also the legislation introduced by Representatives Davis and Moran is a good start.

Second, we should increase incentives for companies to allocate the necessary funds to upgrade their IT security. Today's interdependent electronic economy, a failure of security in one area, can spread to encompass numerous other institutions in a very short time.

Third, we should renew our emphasis on security research and development, especially in developing secure and stable software for our critical tasks.

Finally, we should work together to continue to develop, expand and professionalize the cadre of IT security professionals practicing today. Currently, there are few widely accepted standards defining what an IT security professional knows and does. There's also a dramatic shortage of qualified IT security professionals.

In closing, I would like to reemphasize what is perhaps the most important point of my testimony today. Security is not a static goal that we can ever fully achieve. Rather, security is a continual journey. There is no technical or procedural silver bullet that will magically solve all security issues. Rather, good security is a constantly evolving spectrum of processes, technical tools, policies, and human values that is continually changing and being updated to meet new threats and risks. Only by effectively emphasizing all aspects of this spectrum can we maximize the security and integrity of our national information infrastructure.

Thank you again for the opportunity to share my thoughts with you today. I'll be glad to answer any questions.

[The prepared statement of David Morrow follows:]

PREPARED STATEMENT OF DAVID MORROW, MANAGING PRINCIPAL, GLOBAL SECURITY AND PRIVACY CONSULTING PRACTICE, EDS

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to testify before you today. My name is David Morrow and I am the Managing Principal for the Global Security and Privacy consulting practice of EDS. I have over 25 years of experience in the information technology ("IT") field as a computer programmer and analyst, operations chief, security officer, investigator, and consultant. Prior to joining EDS I was a security consultant with Ernst & Young LLP and Fiderus Strategic Security and Privacy Services, a small start-up consulting firm. I also spent 13 years of a 22-year Air Force career as an investigator of computer crime for the Air Force Office of Special Investigations (AFOSI). When I retired in 1998, I was the chief of the computer crime investigations and information warfare division for AFOSI. I am honored for this invitation to present to the Subcommittee EDS' views on the state of IT security in U.S. industry.

The tragic events of September 11 have brought many changes to our way of life. Along with changes to the physical security of public places such as airports and sports venues/arenas, we have witnessed a dramatic increase in attention being paid to the security of what EDS chairman and CEO Dick Brown has referred to as today's economic currency: knowledge and information.

Although media attention to cyber attacks has increased in recent months, the fact is that commercial and government computers have been under daily attack for many years. However, over the past several years, the frequency and severity of cyber attacks against both government and commercial infrastructures have increased dramatically.

While many, if not most, attacks are relatively minor, such as web site defacement and simple harassment, others are designed to cripple, damage, or destroy the computer networks they encounter. For example, our own EDS network infrastructure detects and destroys over 20,000 viruses, worms (programs that spread through a network by reproducing and transmitting themselves to other network systems), and network attacks per month.

Over the past several years, cyber attack software such as worms, viruses, and hacking tools have become both more sophisticated and easier to use. A computer novice can now download and launch computer attack software as easily as launching a commonly used commercial product such as a word processing program.

Although massive attacks against the national information infrastructure, the so called "electronic Pearl Harbor", have long been predicted and expected, such attacks have, for the most part, failed to materialize. In the current war against terrorism, however, the stakes have risen considerably. A massive, coordinated denial of service attack or a fast spreading program like the recent Nimda worm could have devastating effects on our economy, especially if the attack were designed to introduce random changes to various pieces of data on every system it corrupted, as opposed to simply slowing or halting the system itself.

Our economic system is based upon trust—trust between trading and investing partners . . . trust between consumer and merchant . . . trust between supplier and purchaser. If this sense of trust were damaged or destroyed our economy would be crippled. Maintaining these trust relationships is one of the most important things we can do to insure the continued development and growth of the information economy.

For many years, practitioners of IT security have worried about the lack of both a sense of urgency and priority for corporate IT security. Prior to September 11, companies often viewed IT security as a variable, discretionary expense that lacked a clear benefit to offset the costs involved. This was especially true in companies in nonregulated industries where no clear mandatory standards forced a minimum degree of security planning and structure. Since September 11, however, we have seen a doubling in requests for information about IT security, especially in the areas of business continuity planning and overall security best practices. Tragic as they were, the events of September 11 helped to drive home the fact that security should be considered an essential capital investment rather than simply an expense.

Overall, I would characterize the state of IT security in industry as poor and struggling to improve. New technical vulnerabilities and threats, such as viruses and worms, are released on a regular basis. Many organizations, both in and out of government, still leave the bulk of the work of securing their systems to individuals who perform these critical tasks as an addition to their normal jobs. Because of this, critical security duties, such as making sure software is properly updated with the latest security patches, is a low priority, if it is done at all.

The bulk of the problem remains rooted in a lack of continuing, process oriented attention to basic security principles such as good password practices, tracking and installing critical software patches, as well as user training and education on security basics. According to the federal computer incident response center, about 90% of successful attacks are caused by the lack of updated software patches.

A striking example of this is found in the fact that the Code Red worm, which wreaked havoc on numerous corporate systems a few months ago, took advantage of computer vulnerabilities that had been identified and corrected by a software patch months before. The patch had simply not been installed in many of the machines. Another example can be found in the ease with which many web sites have been vandalized by exploiting well-known and documented flaws in web server software.

Finally, while we have seen a laudable increase in spending on many aspects of physical security, there appears to be little increase in funds allocated to strengthening the security of the commercial information infrastructure which fuels our economy. While many companies are attempting to increase security on their own, the approach is piecemeal as there is no incentive from the government for companies to coordinate their efforts with their industry partners, suppliers, and customers. Such incentive is vital, especially in the current economy.

What can be done?

First, we can concentrate on developing a more coordinated program of industry/government cooperation that stretches beyond the critical infrastructures designated by Presidential Decision Directive 63 to encompass a wider variety of companies and institutions. Programs such as the FBI's Infragard are a good start, but more needs to be done to bolster the commercial sector's level of trust in the government. As an investigator of numerous network attacks, I can attest to the fact that coordinated information sharing among victims of an attack is essential to halting the attack and identifying the attacker. Companies should not be penalized for acting together for the common good. Legislation introduced by Representatives Davis and Moran is a good start.

Second, we should increase incentives for companies to allocate the necessary funds to upgrade their IT security. In today's interdependent electronic economy, a failure of security in one area can spread to encompass numerous other institutions within a very short time. Security of all networks should be viewed as something we do for the good of society as a whole rather than as a discretionary cost to be reduced or eliminated when times are difficult. We believe that the 30 percent bonus depreciation provision included in the House-passed economic stimulus bill

would be a big help in this regard. We also think measures that specifically target investments in security and technology, such as those introduced by Representatives Weller and Upton, would be very helpful.

Third, we should renew our emphasis on security research and development, especially in developing secure and stable software for our critical tasks. A permanent extension of the research and development tax credit could be part of the solution here.

Finally, we should work together to continue to develop and professionalize the cadre of IT security professionals practicing today. Currently, there are few widely accepted standards defining what an IT security professional knows and does. Given the critical role these professionals currently play in our society, we need to insure that we have only the best and most trustworthy individuals guarding our systems.

As a last point, I would like to reemphasize what is perhaps the most important point of my testimony today. Security is not a static goal that we can ever fully achieve. Rather, security is a continual journey. There is no technical or procedural silver bullet that will magically solve all security issues. Rather, good security is a constantly evolving spectrum of processes, technical tools, policies, and human values that is continually changing and being updated to meet new threats and risks. Only by fully utilizing all aspects of this spectrum can we maximize the security and integrity of our national information infrastructure.

Thank you again for the opportunity to share my thoughts with you today.

I will be glad to answer any of the Subcommittee's questions.

Mr. STEARNS. I thank the gentleman.

Ms. Davidson?

STATEMENT OF MARY ANN DAVIDSON

Ms. DAVIDSON. Mr. Chairman and distinguished members of the subcommittee, thank you for the opportunity to address you today.

I'm Mary Ann Davidson. I'm the Director of Security Product Management for Oracle Corporation. Oracle is the second largest software company in the world, and we are a large provider of secure information management systems to both commercial and governmental customers. A number of our customers are involved in national defense or intelligence activities.

Information was on the ascendancy long before the horrific events of September 11 became seared into our national consciousness, and information security remains in our thoughts as we now move to strength our defenses. As ghastly as attacks on our physical infrastructure have been, how enticing would it be to our Nation's enemies to attack our critical infrastructure from cyberspace, where there are no borders, and evildoers can attack us from virtually anywhere, via a computer and a modem?

The information security explosion began several years ago and has accelerated with the growth of the Internet, which has been good news for providers of secure systems and those who depend on them. As more companies have embraced the Internet, security has moved from an afterthought to an essential part of business infrastructure. In that sense, the commercial world is merely catching up to the U.S. Government in terms of the importance it places on information security. Prior to the Internet, the requirements for strong information security were almost solely driven a select set of "professional paranoids," and I mean that kindly, such as intelligence agencies, the Department of Defense and financial institutions. These organizations have understood for years that information security is central to their operations; they are literally out of business without it. For organizations only recently joining the ranks of the security-aware, for example, by becoming ebusinesses, the threat that one's mission-critical systems—now exposed to cus-

tomers and partners—could be compromised has clearly elevated security on their radar screens.

The good news in cyber security is that, while there is still no magic bullets—that's a popular phrase today—there are many steps that companies, whether they're suppliers or consumers of information technology, can take are taking to protect themselves. It's important to note, however, that both consumers and providers of information technology have responsibilities.

Consumers of information technology have a requirement to make security a purchasing criteria. I'm sure you're familiar with the expression that if you don't vote, you lose the right to complain about the election afterwards. This is also true in security. If you do not make it a purchasing criteria, you lose the right to complain afterwards if you've been hacked.

The other thing that consumers need to look for is independent attestations to the security-worthiness of a solution. And there are, in fact, international standards of what it means when you say you're secure. For example, the International Common Criteria, which is an ISO standard, lays out the requirements for vendors of secure products to have their solutions verified by independent third parties. That way it is not merely the vendor's say so that they are secure. And, in fact, no vendor will stand up and tell you that they have a security hole big enough to drive the QE III through. They'll all say that they're secure.

The government has long recognized the value of independent third party attestations, and in fact there are directives which require people to procure products that have been independently evaluated, such as NSTISSP No. 11. I think it would be important to bring something like that, which I believe goes into effect July next year, forward in a post-September 11 world.

It's also important for the government not to deviate from these requirements. Every time sometime grants a waiver on a Federal procurement, you're effectively saying we said security was very important, but we didn't really mean it. There are many vendors who do provide evaluated product, and I think it would be important for the government as a large consumer of secure information systems, to get what they pay for.

Vendors, of course, also have many requirements to provide better cyber security. One of them is to commit to a secure product life cycle; that means everything from building security into your engineering process because you can't add it after the fact, to being very aggressive in treating security vulnerabilities and notifying a customer base when there are problems in our product suites.

Commitment to standards is also important. The more that security is easy to work with and fits together cohesively, the more widely deployed it will be and the better it will work. By cooperation on industry standards, it will facilitate the delivery of secure products and it will give consumers better choices. You don't get good products in a monopoly market. The more that there are standards, the more strong security providers you can have, the more secure will be the result in systems.

Vendors also have a responsibility to think like hackers. Hackers, 98 percent of whom really just want bragging rights when they break into your system, they don't intend to use the information

maliciously. It's important for companies to use that type of thought processes to defend their own systems, very much like the Department of Defense conducts war games.

Another requirement among vendors of secure systems is to join industry ISAC. As the expression goes, either we hang together or we shall all hang separately. And typically when someone does break into your system, they will try the exact same tact on someone else's system or someone else's product. So it's really important to cooperate. And I believe members of the ISAC are represented here today.

In conclusion, I would like to remind you—I guess I'm quoting you Mr. Chairman quoting me—but as with liberty, the price of security is eternal vigilance. We all have a responsibility to pay attention to it and to continue to elevate it our consciousness.

Thank you for your time. I'll be happy to answer any questions.

[The prepared statement of Mary Ann Davidson follows:]

PREPARED STATEMENT OF MARY ANN DAVIDSON, DIRECTOR, SECURITY PRODUCT MANAGEMENT, ORACLE CORPORATION

Representative Stearns, distinguished members of the House of Representatives: Information security was on the ascendancy long before the horrific events of September 11 became seared into our national consciousness, and information security remains in our thoughts as we now move to strengthen our defenses. As ghastly as attacks on our physical infrastructure have been, how enticing would it be to our nation's enemies to attack our critical infrastructure from cyberspace, where there are no borders, and evildoers can attack us from virtually anywhere, via a computer and a modem?

The information security explosion began several years ago and has accelerated with the growth of the Internet, which has been good news for providers of secure systems and those who depend on them. As more companies have embraced the Internet, security has moved from an afterthought to an essential part of business infrastructure. In that sense, the commercial world is merely catching up to the US government in terms of the importance it places on information security. Prior to the Internet, the requirements for strong information security were almost solely driven by a select set of "professional paranoids," such as intelligence agencies, the Department of Defense, and financial institutions. These organizations have understood for years that information security is central to their operations; they are literally out of business without it. For organizations only recently joining the ranks of the security-aware, e.g. by becoming ebusinesses, the threat that one's mission-critical systems—now exposed to customers and partners—could be compromised has clearly elevated security on their radar screens.

The good news in cybersecurity is that, while there are still no security magic bullets, there are many steps that companies—whether they are suppliers or consumers of information technology—can take and are taking to protect themselves. Consumers of information technology need to be discriminating; they must make security a purchasing criteria, and hold vendors accountable through independent proof of information assurance. They must create a "culture of security" within their own organizations, so that security is not diminished by the "weakest link" of a careless or unknowing employee. Vendors of information technology need to cooperate on security standards to facilitate the growth of secure systems, and commit to a secure product lifecycle. Paradoxically, vendors need to both join industry organizations that share information about hacker threats, and embrace the same hacking techniques that expose so many security vulnerabilities (i.e. to detect and mend vulnerabilities in their own products and networks).

In order for any organization to secure their infrastructure, they need to make security a purchasing criteria. Organizations must assess their security requirements—and not deviate from them—as part of system design. If security is not built into a product or system from the get-go, it is often impossible to retrofit it after-the-fact. Organizations also need to look at the total cost of securing a system, including assessing the lifecycle cost of security, such as how often they will have to patch their systems due to significant security vulnerabilities. While no product is bug-free, an ostensibly secure product, for which a vendor is constantly issuing security patches, is a sign that the vendor did not pay enough attention to security dur-

ing design, and at some level does not "get it," or care about security. More importantly, often the single easiest way hackers break into systems is through public vulnerabilities for which the patch has not been applied. A vendor issuing a patch per day or every other day for their product suite is, in effect, building insecure and unsecurable systems.

Industry has begun to recognize the disparate cost of securing products (from competing vendors) through the pricing mechanisms of hacker insurance; products with comparatively poor security track records are priced at a premium relative to their more secure cousins by the companies offering such insurance. For example, one widely-deployed operating system carries a 25% risk premium relative to other commercial operating systems because of the difficulty in securing it. While the government "self-insures" against cyberattacks, the higher risk premium should serve as a signal to the government, as it does to the commercial sector, that a system is riskier and less secure to deploy. Lest we forget the stakes: it is impossible to put a price on national security.

One easy measure of the security-worthiness of products is that of formal, independent security evaluations against objective criteria of "what it means to be secure." There have been many such criteria emerging in the past 15 years, including the US Trusted Computer Systems Evaluation Criteria (TCSEC or "Orange Book"), the UK Information Technology Security Evaluation Criteria (ITSEC), the Russian Criteria, and most recently, the international Common Criteria. The Common Criteria is an International Standards Organization (ISO) standard (15408), and as such, is *the* de facto worldwide standard for independent security evaluations. An independent security evaluation against the Common Criteria is mutually recognized by multiple countries, including the US, the United Kingdom, Germany, and most recently, Israel. This enables a vendor to create a single product "acknowledged to be secure" in many major markets.

The US Federal government has already realized the value of independent security evaluations, as witnessed by the many Federal procurement programs (for example, in the Department of Defense) requiring that a product has completed a formal security evaluation. The National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 requires (as of July 2002), that procurement of commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled IT products to be used on systems entering, processing, storing, displaying, or transmitting national security information be limited to those which have independent security evaluations (i.e. against the criteria outlined above, or the Federal Information Processing Standard (FIPS)-140, which attests to the correctness of cryptographic modules).

Information assurance efforts are undermined by procurement efforts which bypass these directives. Each time a procurement waiver is granted that evades the requirement for evaluated product, it negates the value of information security, and the efforts of vendors who *do* comply with Federal directives. An independent security evaluation of a large complex product, such as a database server, represents about $500,000 of additional security quality control, by someone other than the vendor. Independent security evaluations are the "good housekeeping seal of security," and customers of information security products neglect or negate them at their peril. As the saying goes "you get what you pay for;" the US Federal government, as perhaps *the* largest consumer of secure systems, must demand better security in their procurements and accept nothing less.

An important factor in a strong cyberdefense is the level of awareness of the entire organization—not merely the information technology (IT) department—of the importance of security. The creation of a "culture of security" is a factor in any organization's cyberdefense, for the reason that you can never hire enough "cyberpolice" to secure your infrastructure without the cooperation and awareness of the users of the infrastructure. The best security policy in the world can be defeated by users who are ignorant of their responsibilities under it, or who deliberately flout security policies, much as an alarm system will not protect your home if you leave the door unlocked, or the spare key under the mat. Not every organization requires a culture of security on the order of the National Security Agency; yet every organization has secrets. Creating and enforcing security policies must go hand in hand with employee education and awareness. Most employees want to do the secure thing, but they need to know what it is.

Industry associations such as the IT industry ISAC (Information Sharing and Analysis Center) finds multiple organizations unified against a common threat of cyberattack. Hackers have a nasty habit of repeating prior successes; as one discrete type of vulnerability is exposed, the hack is repeated through similar products from that vendor, or from other vendors. An organization that shares information about a threat to it, whether it is outright attacks on that organization's networks and

systems, or a vulnerability in their product—even at the risk that the vulnerability will be used against it by a competitor—helps strengthen the entire nation's critical infrastructure. As the saying goes "we must all hang together or we shall surely hang separately." Fierce business rivals can and are cooperating in industry ISACS, including the IT industry ISAC. IT ISAC alerts are part of the early warning system for cyberattacks; many of the companies whose products are the foundation of the nation's IT infrastructure are members of the IT industry ISAC.

The cooperation of many vendors upon common security standards facilitates a secure infrastructure in several key ways. One of them is that a protocol that is well-defined and subject to peer review is, all other things being equal, more likely to be secure than one that is proprietary and shrouded in secrecy. "Security by obscurity," the practice of hiding a product's security mechanisms and hoping someone cannot discover a weakness, does not work. Hackers are all too clever at reverse-engineering code and finding security weaknesses. If it's not secure under the light of day, it is not secure at all. Consumers of secure systems should seek security standards-compliant product, as it increases the chances that the security works, and will work with other related products.

Another way in which standards facilitate better security is that it is easier for vendors to integrate security into their products; security is easier to deploy and more widely-deployed when there are common integration interfaces. Finally, the growth and adoption of standards goes hand in hand with market expansion, and this provide consumers of security-related products with greater choice of higher quality products. You just do not get good products in a monopoly market dominated by proprietary security mechanisms, or one in which security solutions are fragmented and do not work together.

An example of this is the growth of public key infrastructure (PKI) a security technology with important applications including network encryption (e.g. via the Secure Sockets Layer, an Internet standard) and digital signatures, which can enable non-repudiation of electronic transactions. The PKI market has been slow to grow, because "I" is the operative word: deployment of a PKI requires *major* infrastructure changes in all products that use it, which has historically been expensive and difficult. Until recently, many vendors of PKI products and services were more concerned with pushing their proprietary technology than cooperating on standards, and growing the market. It has only been with agreement upon and adoption of standards that PKI has been broadly deployable.

Private industry offers many specific cybersecurity technologies that can potentially enable us to better secure other aspects of our nation's critical infrastructure. For example, one of the lessons of September 11 is the necessity of sharing data among interested parties, *real-time,* while preserving "need to know." At the same time, the needs of national security and privacy must be carefully balanced, so that the privacy of all is not compromised to identify the few who are malefactors. For example, "watch lists" could be compared against airline reservation databases, and only those matching records culled and labeled so that those with "need to know" could access them. Suspect names from intercepts from one entity could be centralized in a database, with selected access by other law enforcement agencies. The data, of course, needs to be labeled with appropriate security classifications and compartments, and may be relabeled real-time to facilitate information sharing among greater or lesser groups of law enforcement organizations, intelligence agencies and other parties with need-to-know.

Commercial technology exists today from Oracle Corporation that enables multiple companies' data to be stored in the same database, ensuring that Company A only sees Company A's data, and Company B sees Company B's data. Data may also be accessed by both companies (for example, if they are trading partners), and can be natively labeled with sensitivity classifications (e.g. "Company Confidential: A and B") much like government classifications of fine granularity (e.g. "Secret" or "Top Secret: Project X"). The ability of commercial off-the-shelf software to natively manage data "owned" by different entities, and label data with sensitivity classifications, allows both separation and sharing of data, real-time. We believe this technology to be even more valuable in ensuring national cybersecurity than it is for supporting hosted information systems, exchanges, and "communities of interest" on the Internet, where it is currently used.

The practice of "ethical hacking" is being employed by many companies as a cyberdefense, much as the armed forces conduct wargames. The notion is simple: break into your own systems—or, in the case of software and hardware providers, break into your products—before someone else does. Learning how to think like, and act like a hacker makes it easier to build hack-resistant or hack-proof product. "Lessons learned" from hacking attempts can be used to educate IT professionals and

product developers, as well as continuously improve engineering processes. Ethical hacking is an important weapon in a company's security arsenal.

Ironically, the best cyberdefense for our infrastructure may be the hacking community itself. The vast majority of hackers merely want "bragging rights" among their peers for discovering a security vulnerability; they are not malicious with that knowledge. The more that hackers expose product vulnerabilities and contact the vendors whose products they so creatively break into, giving them time to address the vulnerabilities, the more secure the resulting product is. As much as no vendor likes hackers going after their product, we learn from them and we build better product because of them. It's not too far fetched to think that a "cybercorps" of hackers can measurably help secure the nation's critical infrastructure against the hackers of a malicious foreign power.

There are no security magic bullets. Industry and government, consumers and purveyors of information technology: each must each do his part. The price of cybersecurity, as with liberty, is eternal vigilance.

Mr. STEARNS. I thank the gentlelady.

Mr. Klaus?

STATEMENT OF CHRISTOPHER KLAUS

Mr. KLAUS. Chairman and members of the subcommittee, thank you for giving me the opportunity to testify today.

I'm the founder and chief technology officer of Internet Security Systems. I've been in security for about 10 years. And Internet Security Systems has grown to be a global company and pioneered in the area of intrusion detection, vulnerability assessment, finding a lot of the holes that are on the Internet today. And we put together a team we call X-Force. It's about 100 security researchers who do nothing but examine all the latest vulnerabilities proactively examining various vendors' products. We've worked with several companies that are here on the panel in terms of helping identify issues, working with them to correct a lot of security holes in their products so they can be more robust. And we have a data base of over 10,000 vulnerabilities and threats. So we're kind of like the CDC for computer vulnerabilities.

I guess was looking to address, how have we changed since 9/11. I think, overall, companies are getting more serious about security, but I think there are some other factors that have increased the awareness of security. It's really been the automated attack tools out there, Code Red, Nimba that have proliferated and has had probably the most dramatic effect that I've seen in my history of security in terms of talking to companies where almost company I've talked to has been nailed by Nimba and has been infected all over their network. And one of the ramifications of that has been a shift in probably the leadership within the security groups of large companies.

Probably a year ago or more you'd go into a company and you'd talk to them. And the person in charge of security was somebody whose real technical. He could explain the bits and bytes of security. In the last 6 months we've seen, you know, almost everybody I meet who is charge of security now is somebody who had nothing to do with security in the past, who was a business person focused in on solving the security issue for corporations. And it makes it easier for us, because we're able to talk with them and they're able to translate the bits and bites to getting more resources, putting in the proper policies, etc, for a lot of the companies out there. So we're seeing an increase within the priority of elevating somebody in terms of business.

So it's happening on the private sector, and I think it's also happening within government where we're seeing like Richard Clark being in charge of security reporting up to the President. So that's all improvements.

One of the things that, you know, there's a lot of people screaming "security, security, we need more it." And I wanted to kind of just talk about, you know, how real is the security issue or how real is cyber terrorism.

Last week I was with Howard Schmidt at a conference, and we talked about a lot of the security issues and how real are they. And I think a lot of the automated attack tools like the Nimba, were not designed to be that bad. They were bad, they speak all over, they caused a lot of people to clean up a lot of machines, but realistically without much development cost. If you tried to add in some additional malicious features like after 2 hours of being infected and trying to spread itself, someone could easily make a program to go out and try to erase the hard drives of not only the computer itself, but all the computers on the network.

We're also seeing the capability of sharing very sensitive files. I think SirCam virus would email personal files off your computer to your friends without your permission. And I've had several friends that were like "Oh, my God. I'm glad certain files did not get out." You know, it just happened that it was very limited in number of files.

But with Nabster like program out there, even though Nabster itself is not as popular, there's been a ton of other Nabster like clones out there where if somebody wanted to, they could share lots of sensitive data across the Internet. And to that extent, it would probably take about 2 months to develop a much more malicious attack that utilizes the same capabilities of Nimba, Code Red. So it is very real in the potential that somebody could do that.

Some of the other threats out there we've discussed, such as DNS attacks. The domain name services. When you type in "whitehouse.gov," it uses the DNS service to translate that into basically the IP address. It's like a lookup of all the addresses on the Internet.

All the DNS servers, there's only 13 DNS servers that represent the core root of all DNS servers. So with 13 machines out there, somebody if they were clever, just like they could try and bring down the whitehouse.gov with a flood or a denial-of-service, you could attack 13 DNS servers and bring down the ability to look up addresses on the Internet. And if you can't look up addresses on the Internet, a lot of businesses are going to have trouble communicating with their other partners, etc. So that's an area that could easily be improved on.

And also denial-of-service. We're seeing that, going back to consumers, most of the threat of denial-of-services actually originate from the fact that so many people are logging on to cable modems, DSL servers, DSL modems and the fact that they don't have a personal firewall or any protection on their home computer. And those computers are being infected or compromised in large numbers, and it's very easy to use 10,000 home computers on a cable modem to attack any network in the world and have a dramatic effect on their ability to do business.

Some of the solutions out there that we're seeing companies starting to do. Penetration testing, security assessments. They call up and say, "hey, how do I secure myself?" And, you know, first up in any problem is first the assessment. And so many companies haven't done any kind of assessment. They're rolling out new ebusiness applications on their websites.

We go into banks all the time where on the Internet you can get right in there and basically get into—if you want to talk about identity theft, you can easily steal all the data information right off their website.

The other thing that was kind of surprising to me is about 2 months ago I was at a banking conference. And it was all the IT guys, the guys who really know what's happening in the banking infrastructure. And I was "Like how many people here are doing any kind of around the block, 24/7 monitoring from a security perspective over their network?" So if someone tries to break in and steal credit cards, would somebody notice. And everybody put their head down, because nobody was doing it. And then they looked around and said "Oh, okay, I guess we're not alone in not monitoring the network." So with that, I said how many think within the next 5 years will you be doing monitoring around the clock? And they all raised their hands, and said "Yes, that would be a good thing." So, there's a lot of things out there that people can be doing to improve security. I would say with government, the ISAC are a good movement forward. And I think that within government a lot of times I hear questions about should government regulate security, etc. Probably one of the things that we'd recommend is just working with government to make themselves a good example for others. Because a lot of international governments or governments outside the U.S. are saying what do we do about security and they would like to look to the U.S. Government as a prime example. And right now it's slowly turning around to become better.

So, thank you.

[The prepared statement of Christopher Klaus follows:]

PREPARED STATEMENT OF CHRIS KLAUS, FOUNDER OF INTERNET SECURITY SYSTEMS

My name is Chris Klaus and I am the Founder of Internet Security Systems, known as ISS. ISS is the pioneer and leading provider of information protection solutions. We are headquartered in Atlanta with additional offices throughout the U.S. and international operations in Sweden, Italy, Belgium, England, France, Germany, Japan and Latin America. ISS is a trusted advisor to most large U.S. commercial banks and several government entities. Founded in 1994, ISS has experienced phenomenal growth as we have addressed the critical need for companies and governments to protect their information systems.

Every day, Internet Security Systems stops criminal hackers and cyber-thieves by researching computer vulnerabilities and threats and offering a unique, proactive line of defense for an ever-changing spectrum of threats. More and more individuals are using the Internet for business-to-business warfare and corporate espionage, international cyber-terrorism, or to generally cause havoc and mayhem in our technology infrastructure. ISS dynamically protects online assets through development of the most current protection products available and cost-efficient Managed Security Services. We also monitor networks and systems around the clock (24 x 7 x 365) from the US, Japan, South America, and Europe in our six Security Operations Centers and our Global Threat Operations Center in Atlanta. We search for attacks and misuse, identify and prioritize security risks, and generate reports and analysis explaining the security risks and what can be done to fix them. At the heart of our solution is our team of world-class security experts focused on uncovering and protecting against the latest threats. This team of global specialists, dubbed the X-Force, understands exactly how to transform the complex technical challenges into

an effective, practical, and affordable strategy. Because of all of these capabilities, companies and governments turn to us as their trusted computer security advisor.

THE TRAGIC EVENTS OF SEPTEMBER 11 HAVE HEIGHTENED AWARENESS OF THE NEED FOR CYBER SECURITY. PROTECTION IS NO LONGER A BACKROOM DISCUSSION, AND SECURITY IS NO LONGER SOMETHING BUSINESSES ARE WILLING TO CONSIDER AFTER THE FACT.

The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the nation's most pressing national security issue. Even more likely are cyber attacks aimed at further disrupting U.S. interests and business, or sympathizers with general anti-U.S. and anti-allied sentiments. During the past five years, the world has witnessed a clear escalation in the number of politically motivated cyber attacks often resulting in embroiling hackers from around the world in regional disputes, this to the detriment of the corporations and government networks, specifically targeted or innocently attacked.

Over the course of the last three months, hackers have launched sophisticated attacks, including Code Red II, Code Blue, and Nimda and the Nimda.E attacks. A 2001 industry survey conducted by "Information Security," released on October 16, indicated that out of 2,100 respondents, an overwhelming 89% experienced virus, worms, or trojan breeches in the last three months. This is up from 80% a year ago, even though 87% of respondents had deployed anti-virus software. This indicates the importance of constantly managing the growing and changing threats on the Internet and the growing complexity of corporate and government networks. Moreover, the percentage of those reporting Web server attacks increased over the past year from 24% to 28%. These attacks cost the industry billions in lost productivity and system downtime.

The writing is not only on the wall, it is on the front page of every newspaper in the democratic world, as well as on the minds of corporate officers and directors around the world. The network is the gateway to our assets, and it is the lifeblood of corporations and governments. Quite simply, it must be protected.

The tragic events of September 11 have highlighted the need for increased cyber security. More attention is being paid to detection needed to ward off cyber terrorism. We are seeing this at a policy level here in Washington and in other governments that we serve around the world. The same trend is occurring in state and local governments. We are also seeing it on a demand level in terms of the number of inquiries that are coming into our business. As a result, we are engaging in much broader and more strategic risk management discussions, which include the network and the overall protection strategy for the network.

Information is currency in today's global economy. Any organization with critical information assets stored on a network is at risk. The lone hacker may grab headlines, but industrial espionage, employee sabotage and simple disabling attacks actually constitute the vast majority of attacks against information resources.

These incidents rarely make the evening news, but they add up to additional billions in business losses each year. We pay for these incidents through higher prices for goods and services, lower stock price valuations, increased insurance premiums for online business operations and consumer reluctance to adopt efficient, innovative online business opportunities.

These attacks against information resources are a significant threat to our economic base and our national security. The unfortunate truth is that relatively few organizations are prepared to understand, let alone confront, the threats to information critical for normal business operations. Security specialists are in short supply, and command premium salaries. The cost of this expertise is out of the reach of many organizations. Meanwhile, the dollar losses continue to mount.

It's no mystery how this situation has come to pass. The Internet is designed for rapid, simple communications. That's what allowed it to grow from an academic research network into the World Wide Web, and allowed everyone from individual users to multinational corporations to invent new ways to reach out to each other.

Since security is not part of the Internet's fundamental design, it must be added after an application is written, a system is deployed and/or staff has been trained. In spite of increasing legal, financial and regulatory incentives to invest in security solutions, very few businesses focus on security as part of their core competence. Security measures, therefore, do not receive the attention that other, more profitable business operations demand. Tight budgets and overworked IT staff create an almost irresistible temptation to skimp on security until a crisis occurs.

No one builds a house, then fits the doors for locks after a family moves in. No one adds tail lights and a horn to a car two weeks after it leaves the dealer's lot. And yet, that is exactly how we graft security onto our computer code. We need a

more cost-effective means to protect the availability, integrity and confidentiality of electronic information. We need to make security part of the basic design of our information technology infrastructures.

IN RESPONDING TO OUR CUSTOMERS TO PRIORITY OF PROTECTING THEIR INFORMATION INFRASTRUCTURE, ISS HAS DEVELOPED A COMMON SYSTEM TO MANAGE THREATS AND VULNERABILITIES ACROSS THE ENTIRE THREAT SPECTRUM.

A resounding request from our customers is to deliver systems that incorporate the ability to monitor and protect a broad spectrum of threats across their desktops, networks, and servers. This simplification in the market is being driven by the customers needs to protect the environment with an effective system while understanding that the total cost of ownership is critical to enterprise deployment.

Security is quickly evolving and consolidating into two key foundational elements: inclusion and exclusion. Inclusion represents the security products which allow users to access the resources of a network or a system. These products include authentication authorization and the associated technologies which enable these functions, such as directory management systems, PKI, Smart Cards, tokens, authentication interfaces like biometrics and other forms of authentication.

The second element of security is exclusion, defined as how do I keep unwanted elements off of my system? ISS defines this as protection, and we are leading the way to incorporate a number of innovative technologies into a single common agent to protect the system from the vast array of threats, including threats from content, trojans, worms, denial of service exploits and ultimately misuse by trusted or unauthorized users.

What is needed is better protection, less complexity, lower cost of ownership and 7 x 24 services to augment and assure the integrity of the network and the support of the internal security operations. The ideal solution is a single agent to protect a system from threats, as opposed to several different products from several different vendors, which are not integrated.

To protect themselves from all threats and minimize their vulnerabilities, companies need systems that will prevent and detect security risks at every potential point of compromise on desktops, servers, networks, and gateways. Earlier this year, ISS unveiled the industry's first pervasive protection platform strategy. Our unique product, Real-SecureTM, converges intrusion detection, security assessment, active blocking, and malicious content and code protection capabilities to protect against the converging and broader threat spectrum. Last month, we announced the next major component of our protection platform known as Site-ProtectorTM. As a result of this unified product, customers will be able to control, monitor, and analyze their security protection systems from one central site enabling them to dramatically simplify their security management, reduce their total cost of ownership, and increase the scale of management across broader segment of the network.

AMERICA HAS RECEIVED A WAKE UP CALL THAT CYBER SECURITY IS IMPORTANT AND CAN NO LONGER BE IGNORED.

ISS' vast experience with security breaches has caused us to realize how crucial a secure infrastructure is to the safety and security of our society. Computer security products empower organizations to proactively monitor, detect and respond to increasing network vulnerabilities and threats to enterprise information. These products provide the tools vital for protection in today's world of global connectivity. The public needs to be aware of the breadth of possible security breaches. Government can help realize this goal by focusing more attention and funds on computer security. This includes educating and training the human resources necessary to implement the necessary security measures. Our extensive experience has shown that computer crimes are increasing and will continue to do so. Web sites are an important tool in helping government be more responsive and effective, but they are often a target for computer crime. Web sites should be set up in a secure manner and protected once they are set up. Everyone must learn that protection of our National Infrastructure requires everyone to properly update and protect their system, much like using a seat belt before you leave the parking spot. Government must be seen as a leader in protecting its systems and in assisting corporate and private Americans to do the same. Unless the U.S. invests the necessary resources in this area, America's critical infrastructure will be at risk.

Mr. STEARNS. I thank the gentleman.

Mr. Casciano, for your opening statement?

STATEMENT OF JOHN P. CASCIANO

Mr. CASCIANO. Chairman Stearns, Congresswoman DeGette and members of the subcommittee, I'm very happy to be here today to support your investigation into cyber security in U.S. industry.

My name is John Casciano. I manage the Secure Business Solutions Group for Science Applications International Corporation, otherwise known as SAIC.

As you may know, SAIC is the largest employee owned high tech company in the United States, about $6 billion in revenues. And we support both commercial and government clients around the world.

With your permission I would like to submit my formal testimony for the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. CASCIANO. And I look forward to your questions.

For perspective, I've been involved with cyber security matters for many years in both government and industry. I come from a background of 32 years in the United States Air Force where I had the privilege of commanding organizations that were responsible for developing and operating defenses against cyber attacks, some of which have been reported in the press. Things like Solar Sunrise and Moonlight Maze.

I continue to be involved in Department of Defense cyber security issues today. For example, I served on the 2000 Defense Science Board Task Force on Defensive Information Operations and was also one of the handful of "outside" reviewers on last year's National Intelligence Estimate for Information Warfare threats.

As I mentioned, today I run a business that is oriented in the commercial world. And as you know, for the last 5 years or so we've all exposed to reporting on threats and vulnerabilities to our information infrastructure, and I need not recount them here. Suffice it to say they exist, they are real and have had some impact on the privacy of Americans and on the conduct of American business in the information age. The thing that concerns me is that the security problems, if they are in fact reported at all, tends to be one or 2 day media stories and then they recede into the background, and yet the issues they raise are fundamental to American values and to the future of our way of life and, in fact, our prosperity as a Nation. They represent a legitimate constitutional concern as well as an economic security concern.

Of course, there are lots of reasons cyber security hasn't risen to the level of public consciousness that I believe it deserves. First, it's difficult to understand what I call the—it has a high geek factor. And second, it's not yet resulted in massive losses to individuals or businesses.

The incidents of identity theft, release of private data, theft or proprietary information and impacts on the bottom line is apparently at a tolerable level for most people.

Since our focus today is on business, let me make a couple of comments on the business response. First, many managers aren't really attuned to the problem. Part of the reason is the geek factor that I mentioned a minute ago, but part of it relates to the business case for investing in security. For many managers the problem is tossed to this chief information officer or to the technical staff

to solve, but without the resources or the clout to implement and enforce strong security. Until cyber security becomes a CEO and a board of directors issue, it will not get the attention or the investment that it needs.

In addition, except for some enterprises such as financial institutions, the business case for investing in cyber security either hasn't been made or hasn't been accepted. Every internal investment effects the bottom line, and that's certainly true of the cost of security. If losses due to poor security are generally tolerable, managers will limit their investment.

Second, there's what I call the search for the magic black box, not the magic bullet, the single technology solution to the problem. It's my belief that there is not one there today, nor will there be in any future that I can envision. What needs to be better understood is that good security depends on three interdependent components: People, process and technology. If you don't combine all three, I think you are lacking. I think the national security community understands this, but I'm not sure that business in general does.

The final comment that I'd like to make relates to the rule of government in supporting cyber security in business. First, I think government needs to set a better example of good cyber security practice. This should include steps to maintain and raise the information security posture in departments and agencies over time. They must maintain and expand funding for cyber security, and they need to encourage reasonable standards for security projects and processes. The recent grades assigned to government agencies by the Congress for their 2001 security responses are half grades and are very disappointment.

Second, I think government needs to promote a favorable environment for cyber security. This includes steps to fund key research, more investment in training and education, and the granting of legal relief under the Freedom of Information Act, anti-trust and other regulations which currently impede industry cooperation in the planning and sharing of cyber threat and vulnerability information.

Finally, I think there should be subsidies for cyber protection in industries that are especially sensitive to threats and which are probably least able to defray the cost for cyber protection.

On balance, I'm cautiously optimistic, but much remains to be done.

I look forward to your questions. Thank you.

[The prepared statement of John P. Casciano follows:]

PREPARED STATEMENT OF JOHN P. CASCIANO, SENIOR VICE PRESIDENT AND GROUP MANAGER, SECURE BUSINESS SOLUTIONS GROUP, SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Chairman Stearns, Congressman Towns, and members of the Subcommittee. I am pleased to be able to support your examination of cyber security in US industry and of how industry can effectively protect itself against cyber threats. This is a complex and multifaceted challenge. Today, I would first like to highlight briefly a few of the major threats and vulnerabilities related to cyber security for American businesses, and then discuss approaches the private sector can take at reasonable cost to increase its own levels of cyber protection and assurance. Finally, I'd like to address some steps the Congress could consider in promoting and encouraging an improved cyber security posture for US industry.

For perspective, I have been involved with cyber security matters for some time both in government and in industry. During my 32 years of service in the US Air Force, I had the privilege of commanding both the Air Intelligence Agency and what is now known as the Joint Information Operations Center. In those assignments, I had responsibility for both the Air Force Computer Emergency Response Team and the Air Force Information Warfare Center, and had the opportunity to observe and direct the development of information technology capabilities for both defensive and offensive purposes in support of Joint operations. More recently, while on the US Air Force Headquarters Staff, I participated in developing and managing the response to the real world cyber attacks against the Department of Defense information infrastructure that came to be known as Solar Sunrise and Moonlight Maze. I continue to be involved in Department of Defense cyber security issues through pro *bono work.* For example, I served on the 1999 USCINCSPACE Summer Study on Computer Network Defense and on the 2000 Defense Science Board Task Force on Defensive Information Operations. I was also one of a handful of "outside" reviewers for last year's National Intelligence Estimate on Information Warfare threats.

I retired from the Air Force in 1999, and for the last two and a half years have become involved in cyber security in the private sector, serving both government and commercial clients. Currently, I manage the Secure Business Solutions Group, the information security practice at Science Applications International Corporation (SAIC). SAIC provides diversified professional and technical services that involve the application of scientific expertise, and computer and systems technologies, to solve complex technical problems. SAIC is a Fortune 500 company with annual revenues of $5.9 Billion and over 41,000 employees, and is the largest employee-owned, high-tech company in the U.S.

Within SAIC, the Secure Business Solutions Group provides clients with the full spectrum of information security offerings—consulting, implementation, education and training, and managed services. For many years, SAIC has provided support to the Department of Defense and several civil agencies—including support to the FEDCIRC Incident Reporting and Handling Services—as well as commercial clients. We developed and still have an interest in a commercial security firm—Global Integrity—that created and operates the first Information Sharing Analysis Center, or ISAC, for the financial services industry—as well as ISACs for global firms and for Korea. Today, nearly 40 per cent of my Group's business is for commercial customers concerned with protecting the security, integrity, privacy, and survivability of their business information and that of their clients.

While the terrible events of September 11, 2001 have heightened all our concerns for security and are seen by many as defining the beginning of a new era in U. S. national security, the vulnerabilities—both physical and cyber—have been with us for quite some time. The whole trend toward globalization and the reach brought about by modern transportation and communications have eroded the sanctuary we Americans have enjoyed for over two centuries. These terrorist events have taken both a shocking human toll that we must never let the world forget and an economic toll that has been extremely disruptive to the American people and others around the world. One notable observation from these events is that the cost of entry for such attacks is extremely low. The cost to the perpetrators to plan and mount the attacks was probably less than a million dollars—certainly no more than a few million—while the human and economic consequences have been staggering. The impact of the losses to our economy alone is in the billions of dollars.

For the last several years, we have observed the same low cost of entry for those who would disrupt or attack in cyber space, and the same disproportionate consequences for those who have been attacked. While the impacts of cyber attacks are difficult to quantify, largely due to the reluctance of businesses to report fully, or at all, for competitive reasons, we saw the stock prices of several large companies such as AOL and Yahoo fall significantly as a result of the Distributed Denial of Service attacks in 2000, and some estimates place the recovery and lost business costs at nearly $10 Billion. We have also seen the progress of E-commerce be impeded in recent years over concerns for the security and integrity of transactions, with probable significant impacts on our economic expansion and competitiveness.

More recently, the NIMDA virus was detected and spread within a week of the terrorist attacks. I'm not suggesting a relationship, because we just don't know, but NIMDA represents a new, more dangerous class of virus that operates at a peer-to-peer level, infecting not just servers, but clients and even web pages. The losses from NIMDA—measured directly in disrupted business and in opportunity costs of repair and reconstitution—may well have exceeded several billion dollars despite some early warning by the National Infrastructure Protection Center and the

ISACs. The difficulty in attributing the sources of these attacks and in prosecuting them make them a special concern.

The general sources of these cyber attacks are by now familiar, ranging from the "recreational hacker" on the low end to the more sinister perpetrators from international criminal and terrorist elements and nation-states. Following is a brief synopsis of these:

- **Hackers, Crackers, and Other Outsiders.** These have been the most active source of background "noise" in the cyber environment. They include casual hackers who are often juveniles or "hobbyists" using scripted attacks and commonly available tools from the Internet and its many "clubs." There are also professional level attackers who can design and mount novel attacks against protected targets using both a combination of commonly available tools and "homegrown" capabilities sometimes based on cracking encryption. Their purposes range from joyriding and ego gratification to criminal intent, where fraud or financial theft is the goal. Of interest, the 2001 CSI/FBI Computer Crime and Security Survey indicates among a sample of 186 business respondents that internet connections and outsider activities are now generating the largest source of attacks against the business information infrastructure, more numerous than those due to insiders.
- **Insiders.** One of the most costly and dangerous human threats to business has historically been the insider, and this continues to be the case in the information age as well. Insiders have legitimate access to at least some of the business information resources and IT infrastructure of the enterprise, and often know enough of the company's technology, processes, and human elements to be in a good position to subvert them. They may act maliciously if they are disgruntled employees—sometimes destroying, corrupting, or locking out access to information. On other occasions they may use the system to embarrass the business to the public or use it for financial advantage for themselves and others if they are industrial spies. In every case, they are clear and present threats to the intellectual property, information resources, IT infrastructure, and the reputation of the business.
- **Terrorists and Criminal Elements.** These may be foreign or domestic persons or organizations, and they may launch their attacks through cutouts and indirect network paths from overseas or from within the US. Terrorists resorting to cyber attacks may be advancing a political cause, using direct cyber action to advocate environmental issues; opposing globalization, or attacking modernism on fundamentalist religious grounds. In each case, for them, their end justifies their means. Dramatic, headline-grabbing disruption of the US economy is their goal, and US businesses, especially those that are large and have a global footprint or multinational operations, are attractive targets. Much of the current cyber terrorist activity is low level, to include web site defacement and temporary disruption of business operations. However, terrorism is an activity planned and executed by the alienated, and terrorists and their causes have increasing appeal to students here and abroad who have the skills to become serious cyber threats to business. Of particular concern is the possibility of a combination of terrorist attacks against targeted businesses, wherein cyber, physical, and anti-personnel actions may be taken.
- **State Enabled Threats.** The most complex and difficult threat to combat for both businesses and governments is one that is sponsored and executed with the technology and resources that only a nation-state can bring to bear. Such attacks could be conducted with outsiders, insiders, proxies, or combinations of all three, using leading edge technologies to defeat commercial grade cyber security for even the best-protected enterprises. Businesses that would be logical targets for such attacks would be proprietors/operators of our national infrastructures (e.g., telecommunications, transportation, energy/power, banking/finance, etc) or those large companies that provide key products and manufacturing (defense contractors, chip makers, etc). Unfortunately, the numbers of nations that could conduct such attacks against the US and its businesses are likely to grow, given the low barriers to entry in such warfare. This is warfare based on brainpower—readily available worldwide—and the weapons of choice are computers, fast becoming commodities. State-enabled attacks against U. S. businesses are both a national and economic security threat, and they require vigilance and response by the Federal government, and close cooperation by the business community.

Malicious threats to the information and IT infrastructures of commercial enterprises seek to exploit vulnerabilities in business computer information systems. These vulnerabilities stem in part from worldwide business trends, paths in technology development, and operating standards which affect business processes and decision making:

- **Globalization.** Business is going international as never before and is in a fierce worldwide competition for talent, resources, and markets. Time is money and to the swift belongs victory. Commercial attention is riveted on the business plan, the pursuit of core business, and above all on bottom line performance. Broad connectivity and numerous interfaces both within and without the enterprise are needed to thrive in the "brave new world" of globalization. However, cyber security imposes delays and additional costs of doing business, both of which are unattractive to business leaders responsible for customer satisfaction and the bottom line.
- **Open Processes.** To cut business costs and improve responsiveness, businesses are connecting directly with suppliers and customers, sharing information, and even providing the opportunity for people and organizations outside the enterprise to access and input critical information on production and delivery, purchasing, and marketing. This integration via supplier and customer chains depends heavily on trust and constitutes an inherent process vulnerability, if not addressed by cyber security and other technical and operational checks. Of note, "Information Week Research" issued a study that was conducted this spring among 375 respondents, 67% of whom reported that supply-chain collaboration has increased in the last year. However, only 21% of 4500 security professionals surveyed worldwide by IWR indicate that security policies include procedures for partners and suppliers.
- **Wide Access.** As global businesses concentrate on core competencies, they increasingly rely on outsiders in maintaining and supporting their administrative processes and IT infrastructures. Outsourcing is increasing steadily as a means to cut costs and gain additional business efficiency. Maintainer and outsourcer personnel, a constantly changing parade of names and faces, vetted in uncertain ways in many cases, have insider access to systems and information, and therefore the opportunity to do serious mischief to businesses.
- **Standard Architectures.** Because of the continuing increase in desktop, workstation, and server computing power, the client-server architecture reigns supreme, increasingly supplanting mainframes. Client-server uses standard software in normalized configuration for operating systems and applications; industry-wide protocols for information sharing, display, and storage; and common approaches to design and implementation of system and subsystem interfaces for interoperability in communications and information exchange. Variations in information system design are shunned due to cost and support considerations, even though such variations increase the immunity of the business information systems to cyber attack techniques that target standardized architectures and designs.

Over recent years, the losses to industry from cyber attacks have been real and steadily growing, drawing considerable media attention. The 2001 CSI/FBI Computer Crime and Security Survey reports a 41% increase in electronic financial losses among 186 business respondents compared to a similar sample for 2000. It is a fair question to ask why industry—with or without government support—has not done more to safeguard its information systems and the intellectual property contained within its information infrastructure, and to protect its bottom line. There are several apparent answers:

- **Many managers aren't attuned to the problem.** Cyber security is a consideration for them, but the losses attributed to security lapses are tolerable for many; that is, they view them as part of the cost of doing business. To the extent that managers are attuned to it at all, they generally put the issue into the hands of their Chief Information Officer, who may not have the resources or operational clout to implement and enforce security solutions. The lack of senior management attention is further exacerbated by a failure in current accounting methods to attribute current real costs of losses due to cyber insecurity in business, and to assess the potential magnitude of future losses that could accrue as the cyber threat to business grows.
- **Poor cyber security performance by government.** Starting with the federal government and extending to state and local levels, government "talk" about cyber security has generally far exceeded the resource commitment and management attention it has been willing to devote to the problem of protecting the privacy, integrity, and access to government information and information infrastructure. This judgment has been validated on an annual basis by the House Government Reform Subcommittee on Government Efficiency, which for FY 2001 has awarded government a grade of "F" for its overall cyber security posture. Two thirds of the agencies and departments failed based on the information they are required to provide the Office of Management and Budget. Here, the parallel with the business world is striking, as resources for security solutions are scarce and often considered a problem for the technical staff and not the operational leadership. Fed-

eral jawboning of industry on cyber security has led to a proliferation of advisory and coordinating organizations, but precious little in the way of practical technical support, tailored alerting/warning systems, security incentives, or subsidies to industry to improve cyber protections. In sum, government sets an uncertain example and has provided little help to industry in coping with cyber security issues.

- **The "commons" problem.** Enterprise IT environments are growing, changing, and being used in new ways such as to resist system identification and configuration control. They contain an expanding number of real or potential vulnerabilities in their software, hardware, communications, internal/external interfaces, people, and processes. Moreover, they are frequently subject to decentralized control and resourcing. Everyone depends on them, but nobody owns them. Line organizations do not want to pay for IT, far less cyber security, because of the "free rider" problem in funding the IT "commons" and ensuring its security. Within a business sector, losses due to cyber insecurity may be tolerable if they are judged to be comparable to other costs of doing business, and especially if competitors appear equally affected by the same cyber attacks. The business case for cyber security so far is not well made in businesses outside the financial sector, which necessarily must lead integration of cyber security capabilities into its IT infrastructure based on historic experience with fraud, embezzlement, and theft. Government is waiting for industry to solve the cyber security problem technically, and is waiting too for its shrink-wrapped product solutions. Industry looks upon it as too big, too complex, and too diverse to tackle without government funding and legal relief from public information (FOIA) and anti-trust. The "commons" problem of cyber security will be dealt with over time, either by an insurance approach, by regulation, or by some combination of the two. For now, however, industry does not have the means, authority, or motivation to work a global solution.

Given the threats and vulnerabilities that businesses face, and the tough, highly competitive business environment that keeps management attention on bottom line issues as opposed to security, what can enterprises do to improve their security postures? In developing a suitable cyber security posture for a business, there are certain top-level actions that management must take, and they are independent of the size or resources of the company. In the final analysis, sound security depends on three interdependent elements: people, process, and technology. The elements outlined below are intended to size the requirement for cyber security using the same logical approaches employed for any other business decision:

- **Develop and deploy a sound security policy.** This is a no cost/low cost first step that many businesses fail to take. What is the general approach to security and how will it be addressed and inculcated organizationally? What behaviors and what competencies are expected of users of enterprise IT and information? What will be the standards for access and the levels of information sensitivity? How will management oversight of security be conducted and performance measured over time? How will security lapses be dealt with?
- **Identify critical information, processes, and systems.** What constitutes the major components of the critical IT infrastructure and critical business information, and what levels of protection are required for each? The objective is not to eliminate the threat altogether, but rather to manage it.
- **Analyze threats and vulnerabilities.** What are the real sources of threats and vulnerabilities to the business's IT and information? These are based on business sector experience, state of the world, competition, enterprise footprint, and future business plans. What are the technical, process, and operational vulnerabilities in the IT infrastructure and information resources?
- **Perform risk management.** In examining the combination of threats and vulnerabilities affecting the enterprise IT infrastructure and its information, it is important to make informed and deliberate management decisions about how to deal with risks, consistent with sound business principles. The choices are several, but depend on an assessment of how much risk a business can tolerate versus how many resources it has to commit:
- **Avoid risks.** Take actions that eliminate or do not incur the threat/vulnerability duality of concern in the first place.
- **Shift risks.** Use insurance when available or move liability to others if a threat/vulnerability must be faced. Cyber insurance is a nascent but developing specialty in the insurance industry as work proceeds on identifying risks and developing tools to set premiums.
- **Mitigate risks.** Take technical and/or procedural steps to reduce the threats/vulnerabilities if necessary, economic, and efficient to do. With improvements in security technologies and products, the choices for mitigation are on the rise.

- **Accept risks/develop contingency plans and backups.** Risks that must be run and which are expensive but improbable in occurrence may be accepted if downside plans and alternative approaches can be developed in advance.
- **Revisit and review.** With changes in the threats and vulnerabilities, the whole range of technologies, business processes, people, and IT infrastructure, assumptions and decisions about the level and extent of cyber security must be subject to periodic management reconsideration.

In facing up to the requirements for improved cyber security, there are certain bedrock principles that any business, regardless of size, should consider in developing procedural solutions. They are not technology driven and do not require capital investment as much as management attention.

- **Ownership:** Identify primary and alternate system and data owners to be responsible for identifying the sensitivity and criticality of the information on their systems and validate protection controls and access requirements.
- **Accountability:** Hold individuals with access to information responsible and accountable for protecting information while in their possession.
- **Awareness:** Users are the first line of defense. They should be educated about policies, standards and procedures and adhere to them.
- **Detection & Monitoring:** Implement tools and methods to detect misuse and anomalous activities on both a real-time and periodic basis.
- **Incident Response:** Develop and publish a response plan that details actions required when a violation to the security policy is detected.
- **Defense in depth:** Implement security measures in multiple layers versus single layers, and place security devices as close to the item of value as possible.
- **System Configuration:** System vulnerabilities that can be eliminated without reducing functionality should be corrected. System support devices and data storage should contain only applications or services for which a business reason exists.
- **Assessment/Audit:** Conduct periodic reviews of systems, networks, and applications against policies, standards and procedures to test and measure compliance and determine vulnerability to emerging exploits.
- **Reliable Records:** Maintain secure chronological records and logs on significant activities on the network and critical systems.
- **Recovery:** Implement tools and mechanisms to ensure recoverability and business continuity.
- **Access:** Personnel, systems, or applications should only be granted access rights and privileges based on justified business-related requirements. These rights and privileges must be exercised within the scope and limits of identified responsibilities.
- **Exception:** Exceptions to policies, standards and procedures should be granted or denied based on individual review and management acceptance of risk. All exceptions should be documented.
- **Research:** Investigate, study, and understand emerging security technologies and techniques to develop appropriate methods and controls that protect against ascending threats and vulnerabilities.

The cyber security problem has spawned significant creativity in the development of improved cyber security products by many vendors. Properly selected, integrated, configured, deployed, operated, and supported, these can upgrade the security posture of any business. With increasing attention to and demand for cyber security, and the growth in the commercial cyber security industry, the general classes of security technologies and capabilities below are emerging as shrink-wrapped products which are easy to integrate into IT infrastructures. In parallel, IT product vendors are increasing the direct integration of cyber security functions into their own software lines, making each generation more secure and robust. However, a word of caution! There is a real danger in looking for a single, "black box" solution to an enterprise's security problems. It is my belief that there is not one today; nor will there be in any future I can envision. The combination of people, process, and technology offers the best hope of managing cyber security risks. Some of the more common technologies enterprises should consider are listed below:

- **Perimeter defenses.** Firewall software and devices at the enterprise, network, server, and even host level are becoming standard. These permit a variety of steps to limit access by sender, receiver, domain, function, and data type. Although not the total security solution, these are a necessary portion of the security configuration for business systems, and the first layer in the defense in depth implementation for cyber security.
- **Intrusion Detection.** Unauthorized penetration of business information systems must be assumed. Rapid detection is a requirement. Intrusion Detection Systems

(IDS) work with sensors which either detect (1) specific activities or processes which have been previously templated as threatening, or (2) departures from previous information system activity and behaviors which have been assessed to fall in the "normal" range. New approaches to IDS are beginning to emerge that include combinations of such sensors and detection criteria supported by enhanced data fusion, display, and decision support capabilities. IDS capabilities are improving relative to threat and vulnerabilities, and becoming more widespread.

- **Autonomic Response.** Most IT system response to intrusion and anomaly detection is ad hoc. The next area for improvement will be in automated response to penetration, wherein pre-planned reactions are automatically executed to contain, reduce, and eliminate damage and sources of threat. Over time, development work for DoD may provide for commercialized capabilities for adaptive response to penetration. This area of cyber security products is currently very immature but appears promising for the future.
- **Virtual Private Networks (VPN).** Virtual Privacy Networks provide secure tunnels between trusted sources connected over paths through less trusted domains by using encryption. This approach is mature now and proving necessary for ensuring privacy for businesses using the internet as part of their extended IT infrastructure. In view of globalization and the rise of collaborative working with international partners, VPN technology is a necessary security component for many businesses.
- **Encryption.** Cheap, reliable digital encryption using software has now become available and practical for industry. Software based encryption is susceptible to attack by a state level threat, but is sufficient for all others. Encryption is now required to protect sensitive data in motion (i.e., as it moves through networks and across telecommunications paths) and at rest (i.e., in storage) to ensure integrity and privacy. Encryption is also useful in providing authentication between sender and receiver, and non-repudiation services (for accountability).
- **Public Key Infrastructure (PKI).** Public Key Infrastructure using asymmetric keys has emerged as the only practical technology to support encryption requirements, such as those above, for numerous, diverse users who are geographically dispersed but functionally connected. In a word, this is globalized, 24/7 business today. PKI has been criticized as not being user friendly and scaleable, but outsourced providers can reduce its application to something like a subscriber service for most businesses.
- **Digital Rights Management (DRM).** Digital Rights Management technology provides persistent controls of information and intellectual property over time. It can set and enforce rules for sharing, display, editing/modification, usage, and even expiration of storage. Other DRM capabilities will support secure billing and micro-payments, provide auditing and transaction tracking, and permit alteration in the rules as requirements may change. PKI solutions can provide necessary encryption support. DRM is not yet mature but is an emergent technology that can improve the cyber security of business processes in the future.

I am generally optimistic about the improvements that we see developing in cyber security technology and believe these can be integrated at reasonable cost in ways that will markedly improve protection for individual business IT infrastructures operating in many different business risk environments. These technical safeguards, combined with proper operating procedures and people with suitable training and policy direction, can make business cyber security postures quite robust. Unfortunately, it is also clear that cyber attack tools are improving steadily in their capability and ease of use. We can expect new waves of attack based on widespread internet dissemination of vulnerability information, the advent of adaptive of "polymorphic" viruses, improved counter-encryption capabilities, and clever attack tactics that evade IDS. These attacks will come from an increased number of people globally who are prepared to use cyberspace and sophisticated software tolls in malicious ways. This is particularly of concern as we realize that in the next year the majority of internet content will no longer be in English, and the number of aggrieved foreign players with access and attitude rises.

For the present, the experience SAIC has had as a cyber security integrator with numerous industry customers is a bit mixed.

- Financial sector clients are far ahead of all others in awareness and concerns about cyber security, and in the sophistication of their solutions. They in fact can provide technical and procedural lessons in best practices to the US national security community as well as other parts of the private sector.
- Many of our other commercial clients approach us when they have had a penetration or other IT infrastructure failure. They want quick fixes, some testing to assure the problem has been resolved, and hesitate on cost grounds to support a

longer-term relationship in which their security posture is systematically tested and upgraded.

- In assessing the sources of penetration, we normally find the attacks are not novel, but in fact are familiar. In the majority of cases, patches have been available, but were not implemented. In other cases cyber security systems were not correctly configured. Those persons responsible for cyber security were overworked, under trained, or poorly supported and resourced by their management.
- Many commercial clients are still doubtful about the business case for cyber security and typically do not make high demands on software developers of their operating systems and applications to incorporate strong security features.
- Outside of the financial sector, encryption and PKI are coming more slowly to industry customers than to the Federal government. Government pressures for vendors to use PKI based encryption services in B2G transactions will gradually increase usage patterns. There is some interest in outsourcing cyber security support services and to use managed cyber security service models on a subscriber basis. This is economic, especially for small- and mid-sized firms that are mindful of the cyber security threat, but want to concentrate on their core business competency. Unfortunately, it may take a catastrophic event in cyber space to galvanize business attention fully to cyber security issues and change perceptions about the business case.

Against this background discussion of growing cyber risks, actionable best practices, technology trends, and current business realities, there is an important role for the Congress to play to encourage improvements in commercial cyber security. For good or ill—and I believe for good—we live in the information age, and there is no turning back. While the "dot com" euphoria in the stock market may have come to an abrupt end, the underlying march of information and information technology has not. We are wedded to the cyber realm for our future prosperity in virtually every area. Our challenge is to learn how to live and operate in this new domain. It will take time to evolve public policies and craft information age laws, but progress is being made. In my view, here are some of the things the Congress may wish to pursue.

- Encourage industry to define standards for due diligence in the development and validation of secure software by developers, and its secure implementation and operation by users. In the event these standards were not met they would provide a basis for judicial allocation of liability and compensation. Part of this approach would be to promote security testing of developer's software products according to accepted standards, and to increase emphasis on the integration of proper software configurations with prompt patch updates for operators.
- Advocate an insurance-based solution to appropriate aspects of the cyber security problem that do not lend themselves to "ownership"—the "commons" problem—and an immediate technology solution. As has been proposed in the aftermath of 9/11 for insurers of physical properties, it might be possible to consider Federal backing if insured losses exceeded a certain total due to cyber attack.
- Consider tax subsidies or other incentives for improved cyber protections for certain industries or for the mitigation of particular classes of risks. Low margin industries vital to public welfare in food and transportation, for instance, might be beneficiaries of such support for improved cyber security.
- Support education and training programs for cyber security skills. It does not matter whether graduates of such programs enter government or commercial jobs since their capabilities will benefit business and the nation as a whole. Ideally this would reduce dependence on foreign providers of those skills and services over time.
- Fund certain highly promising cyber security technologies and approaches that are under development. Those that permit information systems to operate in degraded mode despite intrusion, to self-diagnose, and to heal themselves seem especially valuable and promising. However, these technologies are far from ready for a shrink wrapped solution and will require considerable development over time that industry alone will not pursue.
- Resist the inclination to legislate specific technical solutions. As in many similar problems, Congress will serve industry and the nation best by promoting an environment and development of the infrastructure of people and technologies required to define, implement, and upgrade efficient cyber security solutions over time. For reasons I discussed earlier, to fix on any single technical approach now in a field so volatile is certain to fail.

There are bills in various stages of progress in Congress that include provisions promoting improvements in business cyber security practices and capabilities. HR 2435, "The Cyber Security Information Act," and S 1456, "The Critical Infrastructure Information Security Act of 2001," each have provisions to protect from FOIA

requirements and antitrust concerns B2B and B2G sharing of sensitive information for alerting and warning of threats to business information infrastructures. I commend these provisions for your favorable consideration in any legislation that is forthcoming this session.

To summarize, industry faces a future of increasing and evolving threats to its IT infrastructure, Intellectual Property, and other critical information. There is every expectation that better technology is emerging to improve protections. But, more than technology, people at every level of the business enterprise are crucial to achieving upgrades to cyber security. To be effective, managers must provide—first and foremost—competent, executable security policy. That policy must be implemented in specific processes and technologies. Cyber security must become an integral part of business operations. People at the management level need to believe there is a business case for IT security and manage accordingly, and employees must receive training that maintains both security awareness and competence as a sustaining activity in their careers.

I thank you for requesting SAIC's views on this important matter, and I would be pleased to answer any of your questions.

Mr. STEARNS. I thank the gentleman.

Mr. Schmidt for your opening statement.

STATEMENT OF HOWARD A. SCHMIDT

Mr. SCHMIDT. Thank you, Mr. Chairman, and the subcommittee. I'd also like to request that my full written testimony be submitted in the record.

Mr. STEARNS. In the record.

Mr. SCHMIDT. Thank you.

Mr. Chairman, members of the subcommittee, my name is Howard Schmidt. I'm the Chief Security Officer of Microsoft Corporation. I also have the honor of serving as the President of the Information Technology Information Sharing and Analysis Center or the IT-ASAC, the Information System Security Association or ISSA, and I also serve on the board of the Partnership for Critical Infrastructure Security. I'm also an industry executive subcommittee representative for the National Security Telecommunications Advisory Council.

I've served in the public sector for over 30 years with the United States Air Force, the FBI and local law enforcement. And on September 11, I was in Washington, D.C. for a day long meeting with several senators when I learned of the attacks.

As a current military reservist with Army Criminal Investigations Computer Crime Investigations Unit, I reported to Fort Belvoir, was placed on active military duty for the next month and deployed to work for the Joint Task Force for Computer Network Operations, working with the Department of Justice and the FBI through the NIPC FBI headquarters.

That particular experience built upon the many years in the field have given me the ability to see individuals in both communities, both private and public sector, wage daily battles in a war without silver bullets or black boxes, where there will also be someone trying to exploit vulnerabilities and where criminal hackers are proving themselves to be allusive, diverse and endlessly resourceful.

With this background, I would like to review some problems we face and address the steps that Microsoft takes as an industry leader, and some steps I believe that the government should take to address cyber threats.

The issues posed by criminal hackers are real, cross-platform and costly. The Love You virus of 200 caused an estimated $8 billion

in damages. Ramen and Lion worms, which attacked Linux software used to deface websites and extra sensitive information such as passwords. And the Code Red worm exploited Windows server software. Damage has been estimated in those cases $2.4 billion. The Rhino attacks exploited vulnerabilities in the Solaris operating system to stage denial of service attacks. That damage was estimated as $1.2 billion.

Truly these are genuine weapons of mass disruption, not mass destruction, but mass disruption. Yet, perhaps the most depressing fact in all of these stated attacks there has been no perpetrator that has been caught, absent the incident with the I Love You virus writer who remains free since there were no laws in this country that criminalize those actions.

Those attacks did not occur because the innovative engineers who created the underlying code disregarded security. They occurred because equally innovative criminal hackers worked day after day to find, create and exploit vulnerabilities in the software or in the human nature that gave them new ways to repass on our computers, to steal our data and shutdown our networks.

Microsoft is deeply involved in advancing policies to improve critical infrastructure protection through senior executive leadership, continuous improvement of software development, security response, and coordination with law enforcement.

First of all, we lead from the top. Bill Gates, our Chief Software Architect and Chairman, is a Presidentially appointed member of the National Infrastructure Advisory Council. Craig Mundie, our Senior Vice President and Chief Technology Officer was appointed by the President to the National Security Telecommunications Advisory Council. And on a personal basis, I am deeply involved with the U.S. Government's efforts around critical infrastructure protection, the G8 Subcommittee on Cyber Crime, various United Nations initiatives and including I was a U.S. Industry Delegate in the U.S. Australian bilateral meetings on critical infrastructure protection.

Allow me to mention for a moment some of the things we have done in the direction of our executives. We've created a new program to deal with the patch applications that was cited by my colleagues as one of the issues that faces us in the vulnerability issue.

We're also developing superior code analysis processes to root out subtle flaws that can create vulnerabilities in commercial products.

We're expanding the testing of our software by using independent penetration teams and working closely with third party experts in and outside the government to make these tests work.

In addition, we've created a fully staffed highly effective security response organization which we believe is one of the best in the industry.

Like traditional crimes, cyber crime needs to be opposed with strict criminal laws, strong enforcement capabilities and well-equipped and highly trained law enforces. Yet despite the billions of dollars in damage that we've seen in these network disruptions in the past, writers still remain at large. In this troubled time, we can only expect that some of these may fall under the control of terrorist organizations or hostile nations, and thus we need to ad-

dress the inadequate enforcement of criminal laws and insufficient law enforcement resources.

Law enforcers should receive additional resources, personnel, and equipment in order to investigate and prosecute cyber crimes. These hard working officials are often short-staffed and underfunded. Many also lack the state-of-the-art technology used by hackers, and increased funding is needed to place them on par with those they investigate.

We support the following specific actions. We see a need for increased funding for law enforcement personnel training and equipment.

We support tougher penalties on criminal hackers such as civil forfeiture of personal property used in committing these crimes.

We seek clear guidance from the Sentencing Commission on how courts should punish those convicted felons.

We strongly support greater international cooperation among law enforcers in these times-sensitive investigations.

And we want to have the ability to have ISPs to have the authority to share information voluntarily with the entire government once they see that life or limb is endangered.

We've worked very closely with the authors of the pending Freedom of Information Act reform legislation, and when President Bush signaled his support of this reform, and as President of the IT-ISAC, and I assure you that this simple change could lead many companies to answer the government's request to do more in sharing of security information with the government.

From the international perspective, we need international laws enforcement framework that establishes minimum liability and penalty rules for cyber crime, and common intergovernmental cooperation. Without all this, the computer laws on the laws on the books may wind up being useless when cyber criminals cross international borders.

Let me close by thanking this subcommittee for inviting me to testify. The recent horrific terrorist attacks in New York and Washington were physical in nature. And we were fortunate that terrorists or a random hacker did not further create mayhem by unleashing a corresponding cyber attack, yet this is a risk that we still continue to face. We must take steps now to deter these actions to improve technology: Fully funded law enforcement; tough criminal penalties and continued industry and government dialog and cooperation.

We know that security is a journey, not a destination, and by working with our industry peers including some of my distinguished colleagues here, and with the government, we have a chance to keep pace and hopefully get ahead with the cyber criminals and cyber terrorists.

Thank you, and I'll be happy to take questions.

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

PREPARED STATEMENT OF HOWARD A. SCHMIDT, CHIEF SECURITY OFFICER, MICROSOFT CORPORATION

INTRODUCTION

Mr. Chairman and members of the Subcommittee, my name is Howard Schmidt. I am the Chief Security Officer at the Microsoft Corporation. As such, I am one of

many who are responsible for the development of a trusted computing environment at Microsoft and, to the extent possible, throughout the information technology industry. I serve as president of the Information Technology Information Sharing and Analysis Center (IT-ASAC), which coordinates information sharing on cyber vulnerabilities among information technology companies and the U.S. government. I serve on the board of the Partnership for Critical Infrastructure Security, a cross-sector, cross-industry effort supported by the National Security Council and the Department of Commerce. I am also an industry executive subcommittee member of the National Security Telecommunications Advisory Committee. I served for several years in the United States Air Force, the FBI, and local law enforcement, and on September 11th I arrived in Washington, D.C. for one stop among many that would take me across the globe. I was meeting that morning with several Senators when I learned of the attacks, and I immediately reported for duty at the Pentagon. There I stayed for the next several weeks after being called to active duty with the United States Army. During that time I was deployed simultaneously to the Joint Task Force for Computer Network Operations, the Department of Justice, and the FBI's National Infrastructure Protection Center.

That experience built upon my many years of computer security work in the public and private sectors, in which I have observed extremely talented and committed individuals in both communities wage daily battles in a war without silver bullets, where there will always be some vulnerabilities, and where the criminal hacker has proven itself elusive, diverse, and endlessly resourceful.

With this background, I would like to review some problems we face and address two elements of cyber-security. First, the steps Microsoft takes as an industry leader, and second, some steps I believe the government should take to stop cyber-crime.

THE PROBLEM

Mr. Chairman, the information technology revolution has transformed the way business is transacted, government operates, and national defense is conducted. Those functions depend on an interdependent network of physical and technological critical information infrastructures that industry and government work together constantly to secure. Protection of these systems is essential to government and to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, information technology and emergency services sectors—the so-called critical infrastructures of our economy.

These sectors are national assets. Their loss or degradation would severely impact our national defense and the very stability of our economy. Yet, unlike other national defense assets, they were largely built, and are owned and operated, by the private sector. That is why this Administration and its predecessor have insisted that securing critical infrastructures requires a partnership between government and industry. Voluntary cooperation and industry-led initiatives will work best to address computer security issues.

The issues posed by criminal hackers are real, cross-platform, and costly. The *"ILOVEYOU"* virus of 2000 caused an estimated $8 billion in damages. The *Ramen* and *Lion* worms attacked Linux software to deface websites and extract sensitive information such as passwords. The *Code Red* worm exploited Windows server software to deface websites, infect computers, attack other websites, and make computers susceptible to attack by third parties. Damage has been estimated at $2.4 billion. The *Trinoo* attacks exploited vulnerabilities in the Solaris operating system to stage distributed denial of service attacks against several prominent websites. The damage was $1.2 billion.

Truly, these are genuine "weapons of mass disruption." Yet, perhaps the most depressing fact in all of these attacks is that no perpetrator has been caught with one exception—the *"ILOVEYOU"* virus writer remains free since the law of his country did not criminalize his actions.

These attacks did not occur because the extremely innovative engineers creating the underlying codes disregarded security. They occurred because equally innovative criminal hackers worked day after day to find, create and exploit vulnerabilities in the software or in human nature that gave them new ways to trespass on your computers, steal your data and shut down your networks.

ELEMENTS OF A SOLUTION: MICROSOFT AND CYBERSECURITY

Leadership. We at Microsoft are deeply involved at the national level and within the information technology sector in advancing policies to improve critical infrastructure protection. This takes form through senior executive leadership, continuous improvement in software development, security response, and coordination with law enforcement.

First of all, we lead from the top. Bill Gates, our Chairman and Chief Software Architect, is a presidentially-appointed member of the National Infrastructure Assurance Council (NIAC). The NIAC is intended to advise the President and encourage cooperation between the public and private sectors to address physical threats and cyber threats to the Nation's critical infrastructure.

Craig Mundie, Microsoft's Senior Vice President and Chief Technical Officer for Advanced Strategies and Policy, was appointed by the President to the National Security Telecommunications Advisory Council (NSTAC). The NSTAC advises the President on policy and technical issues associated with telecommunications.

Steve Lipner, Microsoft's Lead Program Manager for Security, serves on the Congressionally-mandated Computer Systems Security and Privacy Advisory Board.

Finally, I am deeply involved in U.S. government, G8, United Nations and state & local cyber-security initiatives. In addition to my duties at the IT-ISAC and NSTAC, I recently participated in a U.S.-Australia bilateral meeting on critical infrastructure protection led by the U.S. Departments of State and Commerce.

From the top down, our senior executives believe in excellent security. They drive our thinking on what we need to do to create a more secure Internet infrastructure, and they simultaneously play a leading role in shaping the general U.S. technological and policy environment.

Service & Development. Allow me to mention several examples of what we have done at their direction. About four weeks ago, we rolled out the Strategic Technology Protection Program (STPP) which addresses the patch application problems while also enhancing our software development practices.

As part of this initiative, we are doing several things, including deploying many of our personnel to our customers' sites to assist them in utilizing our patches. We also are providing advanced training to our own developers so they better understand current threats and vulnerabilities; we are developing superior code analysis tools to root out subtle flaws that can create vulnerabilities; we are expanding testing of our software by using independent penetration teams; and we are working closely with third party experts in and outside government.

In addition to the STPP, we have created a fully staffed, highly effective security response organization. We believe that it is the industry's best such organization. It investigates thoroughly all reported vulnerabilities, then builds and disseminates any needed security updates. In 2000, for instance, we received and investigated over 10,000 reports from our customers. Where we found vulnerabilities—as we did in 100 cases—we delivered updated software through well publicized web sites and our free mailing list to 200,000 subscribers.

Another major element of our protection efforts focuses on incorporating new security features in our products. As examples, we have integrated previous stand-alone patches in products like Outlook 2001, installed a personal firewall in Windows XP, and added software restriction policies to Windows XP to allow administrators to limit what software can run on the system.

The feedback we have received thus far from our customers, outside analysts and the press has been overwhelmingly positive. We consider that an essential vote of confidence in the direction we have taken, and these programs are not one-time initiatives. We take them very seriously, for security and privacy go to the heart of our culture.

Education. Leading by example is one way to improve computer security. Making sure that it becomes a national ethic for business and government, however, requires serious, sustained efforts to educate our colleagues in both the public and private sector.

Like any real solution to reducing computer security vulnerabilities, this requires that both sectors play a part. On the industry side, we strongly support industry-generated efforts to spread the gospel of cyber security. At Microsoft, we have done this through the good works of our top executives and through other broad-based efforts to encourage appropriate security practices. For instance, at an industry-wide level, Microsoft this month sponsored its second annual Trusted Computing conference at our Silicon Valley Campus. This conference brought together leaders from industry, government, the academic community and other interested parties to discuss and reach consensus on issues of security and privacy. One of the highlights of this year's event has been a debate about the handling of product vulnerability information. With several other companies, we have taken a leadership position that the public release of "exploit code" by "security researchers"—that subsequently can be used by hackers to break into customers' systems—is harmful to customers and inconsistent with professional responsibility. We believe that similar efforts to reach consensus within the industry can improve both security awareness and lead to real security improvements.

On the government side, I admire and support the job Dick Clarke is doing as the President's cyber security advisor and coordinator. He has worked tirelessly for years to bring the message of computer vulnerability and the need for increased computer security to the nation's boardrooms and cabinet offices. He needs support throughout the government in making clear that this is a national priority. Certainly this message has reached the Department of Defense, which so heavily relies on information technology to gain battlefield superiority. It must become part of the lexicon of many other government agencies and officials.

Criminal Enforcement. Like traditional crime, cyber-crime needs to be opposed with strict criminal laws, strong enforcement capabilities, and well-equipped and highly trained law enforcers. Yet despite the billions in damage and significant network disruption, many criminal code writers remain at large. In this troubled time, we can expect that some may fall under the control of terrorist organizations and hostile nations, and thus we need to address the inadequate enforcement of criminal laws and insufficient law enforcement resources.

To slow this growing threat, penalties for cyber-crime should be increased and law enforcement capabilities should be enhanced. The Computer Fraud and Abuse Act and other statutes make hacking, unauthorized access to computers, and the theft, alteration, or destruction of data federal crimes. However, penalties are weakly enforced, and tougher sentences need to be imposed to deter and punish cyber criminals.

Law enforcement should receive additional resources, personnel, and equipment in order to investigate and prosecute cyber-crimes. These hard working officials are often short-staffed and under-funded. Many also lack the state-of-the-art technology used by hackers, and increased funding is needed to place them on par with those they investigate.

Finally, cyber-criminals and cyber-terrorists operate across international borders, as in the "ILOVEYOU" virus, the "Solar Sunrise" attack, and the "Anna Kournikova" virus. Enhanced international law enforcement cooperation is a vital tool our law enforcers need to fight and find the cyber criminals and cyber-terrorists.

That's why Microsoft strongly supports adding new cyber-crime provisions to the anti-terrorism laws and the criminal code. We see a need for increased funding for law enforcement personnel, training, and equipment. We support tougher penalties on criminal hackers, such as civil forfeiture of personal property used in committing these crimes, and we seek clear guidance from the Sentencing Commission on how courts should punish these convicted felons. We strongly support greater international cooperation among law enforcers in these time-sensitive investigations. And we want ISPs to have the authority to share information voluntarily with the entire government once they see that life or limb are endangered.

We have also worked closely with the authors of the pending legislation to provide an exemption from the Freedom of Information Act (FOIA) for cyber security information voluntarily shared with the federal government. In a letter to the NSTAC, President Bush signaled his support for this reform and as President of the IT-ISAC, I can assure you that this simple change will lead many companies to answer the government's urging that they provide much more computer security data to the government. When that happens, the government network administrators will learn much more about network vulnerabilities from the private sector and be in a far better position to secure their own networks. They will also be able to model future attacks and position themselves to anticipate them in advance, whereas today most analysis occurs after the attack.

Finally, the Council of Europe has completed negotiations on a comprehensive cyber-crime treaty. We know that from an ISP perspective it contains a number of controversial or vague requirements affecting both privacy and regular business practices. We share many of these concerns and worked in several industry coalitions to ameliorate them. Yet we see the clear need for an international law enforcement framework that establishes minimum liability and penalty rules for cyber-crime, and common procedures for intergovernmental cooperation. Without this, all the computer crime laws on the books are useless when cyber-criminals cross international borders. Whether or not the Council of Europe treaty is an ideal vehicle I leave to the lawyers to decide, but I assure you that we do need harmonization and cooperation in this area, and we need it now.

Investment. Microsoft believes that there is a demonstrated need to protect and defend the nation's critical information infrastructures from computer hackers and cyber-terrorists. Law enforcement must be adequately trained and properly equipped to fight cyber-crime, whether it is hacking, or other forms of cyber-security offenses, committed by terrorists and other criminal entities. That is why we propose giving the Attorney General additional discretionary funds to expand staffing,

training and technological capabilities of the Computer Crime and Intellectual Property Section and the National Infrastructure Protection Center; to accelerate funding for law enforcement computer modernization; to hire experts in cyber-security; and to fund state and local law enforcement efforts to deter, investigate and prosecute cyber-security offenses.

Government Response. Software security is a rapidly evolving market of suppliers and consumers. We have seen over the past few years tremendous growth and a massive increase in awareness of these issues. There is no single nor comprehensive solution and there will always be more to do. For this reason, I believe we need to let the Internet economy and the information technology industry operate as a market. That means that it must operate without government interference.

Federal security mandates or requirements, such as rules and regulations for patch application, dictates on the type of technology a company must use, or legal requirements that a company declare that it follows some form of security best practices, would have the perverse effect of slowing innovation in the security market. A rule requiring notice of security practices would also have the unintended consequence of causing companies to gravitate toward accepted practices rather than toward innovative practices. In sum, there is a critical difference in quality, innovation and thoroughness between security solutions driven by market and private sector pressures and those driven by regulation, bureaucratic timetables and one-size-fits-all approaches. A serious government-industry partnership can encourage security innovation and implementations, but will falter if regulation is imposed upon information technology businesses.

SUMMARY

Let me close by thanking the Subcommittee for inviting me to testify. Although the recent horrific terrorist attacks in New York and Washington were physical in nature, Congress quite rightly must look beyond the current tragedy and loss of those catastrophic attacks. We were fortunate that the terrorists or a random hacker did not unleash a corresponding cyber attack. Yet that is a risk we face, and we must take steps now to deter these actions through improved technology, fully funded cyber crime law enforcement, tough criminal penalties, and continued industry & government cooperation. We know that there is no finish line to these efforts, but by working as we have with industry peers—including some of these panelists—and with governments, we have a chance to keep one step ahead of cyber-criminals and cyber-terrorists.

Thank you.

Mr. STEARNS. Thank you, Mr. Schmidt.

The committee that I'm chairing now is using the jurisdiction of Commerce to have you here. Some of the things you mentioned, Mr. Schmidt, would most likely be under the Judiciary Committee in terms of the laws that are developed.

But, Mr. Klaus, let me just ask you, I have lots of friends in my congressional district that are banking Bank of America, other banks. They do all their banking through the Internet.

Are you saying today that you could go into those programs and find out what their banking information is? Could I bring you down to Okal, you sit down at a computer or could I tell you where they are? I mean, tell me how would you—first of all, is it possible for you, is it possible for a hacker today to go in and find out all the information in my friend's banking account with Bank of America?

Mr. KLAUS. There's actually a pretty big misperception out there where people think that if I don't shop on the line or I don't access my bank account on line, I'm okay. I'm not effected by this. But the reality is when we go into a bank or do what we call a penetration test, we don't have to physically go anywhere, we could just do it from anywhere on the Internet and typically you can get into a bank. And from there you can access not only the people who do access their accounts on line, but even those that are off line in terms of everybody's—everybody's account information is in the data base.

Mr. STEARNS. Okay. That's why we've always made the agreement on this committee that if we do an Internet privacy, it's off line/online, because just what you said; that you could go in to find something and a person never gave a credit card, never went on banking online, but dealt with a bank offline and paid the mortgage, you could break in today you're saying and do that?

Mr. KLAUS. I mean, the banks use the same computer systems, the same data bases to store the information whether the user's online or not.

Mr. STEARNS. Okay. What's the motivation in your opinion of these people who do this? Is it for crime, is it just for challenge, or what is the majority of the motivation?

Mr. KLAUS. I think the motivation it's probably a bigger different group that's out there today. Like 5 years ago or 10 years ago if you looked at it, a lot of people who were doing it was more for play and exploratory type hacking, is kind of the term they were using in terms of "I'll see what I can get into."

Mr. STEARNS. Sort of as a game.

Mr. KLAUS. More as a game. But nowadays we're seeing a lot more attacks that are actually criminal in nature, either political motivation or actually money—you know, money is on the Internet now, so a lot more of monetary attacks. Blackmail a lot of times.

We were dealing with a bank in Georgia where they had been hacked into and basically the data base of all their customers had been taken back to someplace in Russia and, basically that group had emailed the bank saying, you know, please give me $100,000 otherwise we could be releasing this information, might get out on the Internet.

Mr. STEARNS. So they tried to blackmail the bank?

Mr. KLAUS. Correct. And so we're seeing the motivation is changing.

I think the automated attack tools, the motivation there today nobody—since those people haven't been caught, it's hard to question exactly what they're doing. But in many cases if you look at virus writers, it's kind of like so many arsonists out there. You set a fire and you go off and kind of watch it from afar. And I think that's what a lot of the automated attack pools like Nimba, Code Red, some of that motivation might be.

Hey, let's write a program to see how much of a fire can I create on the Internet, and kind of watch it from a distance.

Mr. STEARNS. Ms. Davidson, you state that "If security is not built into a product system from the getgo, it is often impossible to retrofit it after the fact." You might just elaborate on that.

Ms. DAVIDSON. Well, I think it's important that security has to be part of a design process. And a vendor of a secure product has to make a commitment to a secure product lifecycle.

For example, before you build a piece of software, you need to sit down and say what are the security threats I'm protecting against? What are the technical measures I'm going to implement?

Mr. STEARNS. Can you project that with this technological advancement, this innovation we're seeing in America? Can you be sure?

Ms. DAVIDSON. I don't think you can ever be 100 percent sure and there is no bullet proof security. But it basically gets back to,

I talk to my customers about the questions you ought to be asking all of your vendors about security. And that is, how do you build security? Is it part of the design process? Is that one of the first things you think of? Do you have secure coding practices? do you have a small group of people? Because it's hard to get security right.

You have a small group of people who are the experts to whom the rest of your company goes to make sure I'm building a piece of software, I need to make sure the security people; I talk to them, I use the code routines that are well formed and well delivered, I have testing to test the security mechanisms, I do security risk assessments or penetration tests, try to break into it.

Mr. STEARNS. Yes.

Ms. DAVIDSON. We have a team of reputable hackers whose very good that's breaking into things before the product goes out the door.

Mr. KLAUS. I'd like to add——

Mr. STEARNS. Let me just finish here.

Mr. Schmidt, you've just heard what Ms. Davidson said. Some people have criticized Microsoft plan to work to publicize security flaws, but not the technical details. So there's some controversy here, because people like to know the technical details. You might give us why Microsoft proposed the action it did.

Mr. SCHMIDT. Well, it goes around what we call ethical reporting. There is the concern that if information comes out before there's a fix, then we endanger the entire critical infrastructure that we're talking about on a regular basis to begin with. So when we talk about publishing details, it's after we have the ability as an industry to resolve these problems, that you get the patches out there, and then make that information known on a very technical basis. In the interim we're subject to saying there's a big hole, but there's no way to fix it at this point.

Mr. STEARNS. My last question is to Mr. McCurdy, would an exemption from the Freedom of Information Act and/or any trust laws help promote a better interaction and cooperation between the government and private sector on cyber security matters?

Mr. MCCURDY. Mr. Chairman, yes. I'm a firm supporter, as our organization is, for both the Davis-Moran legislation from the House and also the Bennett legislation in the Senate. We'd like to see both of those tabled so we could go to conference on that.

One for information sharing and—what we don't know is probably a bigger question. I know it philosophical. But when you talk about the motivation of hackers, in a lot of ways they want to have those attacks publicized, but it's the criminal elements, it's organized crime, it's the state actors that quite frankly don't want you to know. And they're not using the automated tools. they can do a number of things both externally but also through insiders. As we know, the FBI knows a lot about the potential threat from insiders.

So there are a number of things, and I think you have to remember that used to use in national security the threat over here and the likelihood of occurrence, but the lesser threat on the other side. Those areas where there's the greatest threat you won't hear a lot

about. And that's why, you know, I think there has to be a lot of effort from the government.

With regard to information sharing, banks have their own incentive to report a certain level of intrusion and loses. they don't want to lose confidence with the consumer or customers. So it's also critical that in order to exchange information with the government, that those reports remain anonymous, that they not be traced back to individuals or to companies. Because that has a chilling effect on the reporting.

And as far anti-trust, whenever you bring companies together—you know, government tends to think in vertical silos the way it's organized. The Internet cuts all through that, so it goes across industries. It's not just a group of people from one industry sitting in the same room together. It's a process——

Mr. STEARNS. I'm going to ask you please to summarize this, because we're going to go back—I'd like to get the rest of the committee.

Mr. MCCURDY. The point is that anti-trust exemption for this similar to the Y2K experience and informing sharing exemptions are important and I think it should be supported in a bipartisan basis.

Mr. STEARNS. Okay. Thank you.

Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman.

Following up on the chairman's question, Mr. McCurdy, I'm wondering if there have been any prosecutions for anti-trust violation as a result of information sharing, or if you're concern is really one of a chilling effect?

Mr. MCCURDY. It's more the chilling effect. Similar to Y2K. Once——

Ms. DEGETTE. Yes, I got you. I don't have much time, as you know better than anyone here.

Is anyone else on the panel aware of any anti-trust prosecutions as a result of information sharing? So what I'm really hearing is we're talking about a chilling effect that could be very real for folks? Just for the record, everyone's nodding their head affirmatively.

I was struck, a couple of a you talked about, including Ms. Davidson, about how important it is for consumers to understand exactly what the issues are because you can't complain if you don't action. And I told the chairman my husband installed protection software on our home PC. And we found that even on the first day we had scores of attempts to break into our PC. And I would be willing to bet—and he was surprised to hear it. I shouldn't tell tales on him. But he was surprised to hear that and asked me for the name of the software, which I'll get him. But if we don't even know that on the subcommittee, imagine how many millions of customers there are out there, and that's not even at a business level. So I think that's advice well taken.

I would like to ask a question of any member of the panel who would care to answer it. If you know of any or if you've learned of any particularly vulnerabilities in security systems since September 11 or if there are really ongoing concerns that we have and

that we've been talking about for quite some time in this subcommittee? Any new vulnerabilities that we learn of?

Mr. MCCURDY. Well, I'll give you a quick site. You can go to a website, and they report continuing vulnerabilities. There's a lot that's—again, because of the technical concerns that Mr. Schmidt raised, you don't want to give out before there's a patch, but there are reports.

Since September 11 there has not been a huge rush of new ones. We're not talking about a post-9/11 scenario here. This is a continuing throughout the year threat the past 4 years, which I think the trend that you're concerned about.

Ms. DEGETTE. Mr. Axelrod?

Mr. AXELROD. The status of the vulnerabilities is not really a function of the threats.

Ms. DEGETTE. Right.

Mr. AXELROD. The vulnerabilities increase as new software which is more complex comes into the marketplace. However, I do believe that everyone's perceptions of threats has changed dramatically. And I also think the reality of the threats has changed. There is a whole portfolio of additional threats that we didn't previously consider.

Ms. DEGETTE. Thank you.

Mr. Klaus?

Mr. KLAUS. I'd add that, well, we've found at least three new vulnerabilities since September 11. A couple of them were like multi-vendor effected. Most of the UNIX platforms, Sun, Linex, etcetera and worked with a lot of the vendors out there that fixes issues.

The thing is, we're working with Microsoft and seven other security companies to create a standard. Right now there's a lack of a lot of security standards for whatever reasons, but right now there's not a standard out there for how to disclose that information.

ISS has come up with a standard that says, you know, we will alert the vendors before we disclose any technical details. and a lot of the debate is whether you release the actual exploit tools. There's a lot of security companies that will produce an exploit tool and say, hey, here's evidence that this is a big issue. The problem is you can take that tool and break into systems.

Even worse though is when you disclose I guess the source code to the actual vulnerability and how to break into systems. What we're finding is it lowers the barrier to creating the next Code Red worm or the next worm. And that has the huge effect. That's what scares me is the fact that, you know, new vulnerabilities get amplified and they're a force multiplier in terms of having a huge effect on the Internet.

Ms. DEGETTE. I got you. Thank you.

I'd like to question of Mr. Schmidt. A couple of the excellent suggestions I thought that you made were increasing penalties for hackers. We apparently have hackers out there who haven't been prosecuted.

I'm wondering how many of the hackers that you are experiencing in your company and maybe Oracle and others have we determined are based domestically here?

Mr. SCHMIDT. Yes, it's really difficult to tell until you actually put the habeas grabis on them, as we call it.

Ms. DEGETTE. Right.

Mr. SCHMIDT. Because they're often times——

Ms. DEGETTE. That's a term of art, right?

Mr. SCHMIDT. Because what happens, we see systems that are compromised in foreign countries which may give the indication that the source is indeed that country, but it could indeed be someone domestically that's using that as a jumping off point.

Ms. DEGETTE. So in essence we don't really have a clear sense of how many of the hackers are based here where we could send in the FBI to get a more local law enforcement authorities and how many are based physically internationally, which would argue for even stronger international cooperation?

Mr. SCHMIDT. That's correct. Yes, ma'am.

Ms. DEGETTE. Yes, Ms. Davidson?

Ms. DAVIDSON. Yes, I'd like to amplify an earlier comment. In our experience most of the hackers, although that tends to have a pejorative connotation, in our experience most of—I would say 98 percent of the people that we deal with are inquisitive, talented and, as I mentioned, really want to test something rights on the Internet. Looky, see, I was the first one to find this vulnerability. They are not malicious. They bring the issues to our attention. They give us a chance to fix them. And we're very good about acknowledging thank you. In fact, I think some of us know the same people, is it Yorgi in Russia whose very good at finding buffer overflows.

So as long as you put a little statement with an acknowledgement to Mr. So-and-so who found this and worked with us to help identify it, they're happy.

Mr. SCHMIDT. Yorgi.

Ms. DAVIDSON. Yes, Yorgi. Everybody knows Yorgi.

Ms. DEGETTE. Unfortunately everybody does not have those kind of——

Ms. DAVIDSON. Yes, that's true. But most of them—so in many cases they do self identify and they're very well known. It's the 2 percent who are malicious that you never know they are.

Ms. DEGETTE. Right.

Thank you, Mr. Chairman.

Mr. STEARNS. Thank you.

The gentleman from Illinois.

Mr. SHIMKUS. Yorgi, alias Nathan Deal. You didn't know that, did you?

Mr. MORROW. I didn't.

Thank you. I'd like to follow up on a couple of questions of Mr. Morrow.

Mr. MORROW. Sure.

Mr. SHIMKUS. And since the Davis-Moran bill was mentioned, I know in your testimony you mentioned it also. I want to know if it's a good idea that there be an obligation to share information?

Mr. MORROW. We don't really believe—I don't believe it's a good idea to have the obligation, because I don't necessarily believe it's required.

I think everybody that I run into in the commercial sector wants to do the right thing. They're extremely cognizant of the idea that we all have to share information. They are, quite frankly, not to be dogging the attorneys in the room, the corporate counsel always advise against it because of the issues of anti-trust and the Freedom of Information Act.

You have to understand that even in the investigative world—Howard and I were investigators together for the Air Force. We would find that companies will forego investigation because they don't want to see the information that they are trying to keep sacred, their intellectual property, for example, brought out in open court and read about it on the front page of the Washington Post. And similarly, they're afraid of the Freedom of Information Act will do essentially the same thing, or the anti-trust implications will be kicked in.

While it has not been that I'm aware of ever been a prosecution of anti-trust based on this type of sharing, it's certainly one of the things that a corporate counsel always seems to be worried about.

Mr. SHIMKUS. Great. Thank you.

And I'm going to shift all over to different things based upon the testimony.

Mr. Casciano, you had also addressed in your statements about the applicability of insurance and how insurance may shift risk and help address liability issues. Can you take us through how this would work, just briefly talk us through that whole insurance?

Mr. CASCIANO. Certainly. There are many ways that this can be done, and the insurance companies and the underwriters are trying to grapple with this now.

One possibility is that companies who are going after cyber insurance would be subject to a very standard and rigorous examination; vulnerability assessment, assessment of policy, implementation of that policy, testing of that policy and then would receive a rating from the underwriters based on their adherence to the standards set by the insurance company.

Mr. SHIMKUS. Is there in the proposal a reevaluation of their proposal at 6 months because of how things move so rapidly?

Mr. CASCIANO. Oh, clearly. And that would be part of the standards that would be applied, whether it be a 3-month revisit, 6 month revisit or some other formula. But it would have to be continuous, because the technology both for defense and for offense are changing every day, literally.

Mr. SHIMKUS. Do you think companies that may offer this might hire your EDA to try to prove them wrong.

Mr. CASCIANO. Or companies that hire Yorgi. The ethical hacker.

Mr. SHIMKUS. Right.

Mr. CASCIANO. The ethical hacker. And several of the companies that are represented here have stables of ethical hackers that do this on behalf of clients.

Mr. SHIMKUS. Great. Thanks.

And I want to go to Mr. Doll for my last question. The newly created Critical Infrastructure Protection Board, do you think this should be codified? In other words, put into statute?

Mr. DOLL. I think the protection board is a positive step forward to get a partnership with private industry and public. And I think

we're positive that it's a step in the right direction, that we need to share information and to move those things forward.

Now, what happens next and how that would play out, I don't think I'm in a position to say how that really effects future decisionmaking. so I think that we're cautiously optimistic right now.

Mr. SHIMKUS. You know, we're legislators here, so our question is always does the Executive Office suffice for now or do we need legislation to codify it? It's evolutionary right now. And I would recommend that if you—it's no different than what we're doing in these other issues of bioterrorism of homeland defense. As we move forward, if there's a time to codify, then please come back.

Did you want to add, Mr. McCurdy?

Mr. MCCURDY. Well, to me a follow up. Yes, I think we're in an assessment period of time. The events of 9/11 have changed how corporations are responding to this. We work with many of the Fortune 500 and now board level responses are coming to this. And I think we need to assess and then act aggressively once we formulate some policy.

Mr. DOLL. I would urge the committee and the Congress to be careful about mandates with regard—and getting in the business of architecting some kind of structure here. Because as soon as you do, then the problem changes.

One of the challenges we in America face, and certainly you as representing the government, is that the government is not organized today and has become too stovepiped and too rigid. And I think Mr. Ridge and others are finding the challenge of that.

So I would think that the best model were to be the voluntary model that was used during Y2K and look at some of the specific legislative efforts to improve the information sharing.

Mr. SHIMKUS. Thank you.

And I yield back, Mr. Chairman.

Mr. STEARNS. I thank the gentleman.

Mr. Deal?

Mr. DEAL. Thank you, Mr. Chairman.

We've been made aware over the last several weeks that some of the same things you're alluding to exist in other areas of government. For example, we are told that FERC, OSHA, other Federal agencies require those over whom they have certain jurisdictional controls to divulge to them the worst case scenarios. In other words, where are your power plants most vulnerable and how? Where are you pipelines most susceptible to being bombed or interrupted.

And by virtue of the government agencies requiring this information, it likewise under the Freedom of Information Act, then becomes available to whoever might want to know what the worst case scenario is and they don't even have to do their own homework, the agency has been forced by the government to do it for them.

Now when we talk about the Internet we, for most purposes, kept our hands off of it pretty well. So I don't see it from that angle, but is it the fact that many of your clients are regulated by existing Federal agencies such as the banking industry is regulated, and therefore if they disclose information it then becomes available as to either problems that have existed or potentially do

exist? Is that same kind of scenario that you are seeing playing out, and if so would somebody elaborate on what it is? Because you mentioned the Freedom of Information Act. I can see it from the standpoint of once you disclose a vulnerability. But are there mandatory requirements in place that require those disclosures or can you as Mr. Morrow said, just maybe simply keep your mouth shut and thereby avoid it? What is that?

Mr. MCCURDY. Well, first of all, Mr. Deal, some of those other agencies, FERC and others, are in heavily regulated industries including telecommunications. Again, that's a sectorized approach. The Internet cuts through that vertical and that stovepiped organization. Eight-five percent or even greater of the Internet's none government. It's publicly owned. And it's hard to impose some kind of regulation or mandate on them.

Grimm-Leach-Bliley was an important tool for the financial industry, but that's—and it's a good standard, but it's not a standard that should be applied all the way across. Eighty percent of the problems of the Internet are common to all industry, whether it's insurance, whether it's the utilities, you know, entertainment industry. That's where we think that by improving the information sharing, by having these horizonal nonprofit private organizations as opposed to government, you will get the greatest flow of information that improves best practices, and that's what you're talking about. Not formal rigid standards, but mandatory practices.

I thought the statement about people processing technology is a good matrix to use. We ought to be focused on the people, and that's what industry ought to be doing. Technology we can do as well. We can cooperate through these public/private partnerships, but I don't believe it should be a rigid government standard.

Mr. DEAL. Several of you, though, have mentioned the Freedom of Information Act as being a problem area. Is any of the legislation that is pending now address that particular——

Mr. MCCURDY. Yes, Davis-Moran and Senator Bennett's bill provide an exemption as in the Y2K exemption for information sharing.

Mr. DEAL. And that should solve most of those problems?

Mr. MCCURDY. I think there's unanimous support here for that position.

Mr. DEAL. Okay. All right. Fine.

I believe we're getting probably close a vote on the floor, from what I understand.

I'll yield back, Mr. Chairman.

Mr. STEARNS. Well, no. We haven't got the 10 minute vote yet.

Mr. DEAL. Okay. Well, let me ask Mr. Klaus, and let me tell you we are proud of Mr. Klaus, a Georgia Tech graduate——

Mr. KLAUS. The Georgia mafia, you got to watch——

Mr. DEAL. As you can tell by his appearance, he is one of the younger more successful entrepreneurs and one of the really leading experts in the area of security, and we welcome you here.

You had a response I think to the earlier initial question that the chairman had asked that you didn't have a chance to respond. Can you remember what the issue was that you wanted to respond to, and I was going to give you the chance to do that?

Mr. KLAUS. It was adding onto a comment, and I did not write it down in terms of exactly what it was going to be.

Mr. DEAL. All right.

Mr. KLAUS. I appreciate that.

Mr. DEAL. I think all of us are concerned about what can we do. We don't want to do anything that's going to make it worse, we want to try to make it better. And I gather from your comments that most of you are supportive of these remedial pieces of legislation that are pending.

Obviously things like sentencing standards and sentencing guidelines are not within our jurisdiction, nor the jurisdiction of the Committee on Civil Forfeitures.

You know, I suppose we would have to forfeit a lot of nerd's computers out there if this is the remedy that's there.

But if we have moved from just the prankster, the intellectual graffiti artist to the more sophisticated people, you've already elaborated on what some of those motives are, whether it be blackmail—which that's an interesting one, I hadn't thought about that one—to actually attempting to actually seize some form of money and the processes that are interchange of commerce, how do we get a handle on that? Because obviously this is the Commerce Committee and we have interstate commerce type jurisdiction whether we can pass it maybe to the Judiciary Committee for their responsibilities or not. But are there other areas of legislative corrections that you envision need to be made that are not embodied in any of the pending bills?

Mr. KLAUS. I would suggest the other oversight responsibility of this committee, which has an incredible breadth of jurisdiction and continue to have the hearings. Don't leave it up to government on the other side to do this.

Government can provide a model, but I would urge you to look at other industries, cross industries. There's some interesting things with regard to insurance.

There are cyber insurance policies today, now they're not based on a lot of actuarial data, because there is very little data. They're kind of seat-of-the-pants, and insurers will tell you that. But there's some interesting contradictions.

For instance, physical coverage for terrorism is now available, but cyber terrorism is not covered under insurance. And the question is are you going to get boards of directors and senior leadership of companies to pay attention if, in fact, it's not. But if you mandate it, then you create a whole potential area of cost.

So there's some tough balances here, and those are very interesting questions that I would submit probably fall within your jurisdiction.

Mr. DEAL. One quick follow up. A lot of you have said the government ought to be the one to set the example by the agencies of the government. And you've also talked about the industry trying to come up with industry type standards.

One of the worst things I think the government does is to do something but do it differently from one agency to the other. Has that begun to happen, and is there any effort now to say if the government is going to initiate security protections, that it should be a uniform type security protection that every agency of the govern-

ment follows the same kinds of standards? Is that happening or is it not happening?

Ms. DAVIDSON. Yes, Mr. Deal, there are some differences. For example, even among the constituency that requires security evaluations, for example, against the common criteria I have seen agency specific what they call protection profiles. So even though there's a common framework for what does it mean when you say you're secure, I have seen a number of agencies who say we want our own special Good Housekeeping seal of approval, even though it may be the exact same product.

Mr. DEAL. And that's for vendors attempting to sell products.

Ms. DAVIDSON. Exactly.

Mr. DEAL. Okay.

Ms. DAVIDSON. And that's very difficult because I would say for a large complex data server, the cost of one of these evaluations is about a half a million dollars plus, including personnel costs, make it a round million dollars all in. And for companies to do that on an unfunded basis is very difficult, particularly in these economic times.

What I'd really like to see is to say if you do it once, it's good across all the agencies or the entities who have an interest in this type of product, and you could take the most discriminatory approach and say we'll make the most rigid standard rather than the least rigid standard the one that companies have to comply with.

Mr. DEAL. So that could be an oversight issue.

Mr. STEARNS. I want to thank the gentleman.

And let me just conclude by thanking all the witnesses for coming this morning and this afternoon. I think it's a very good hearing.

I think the conclusion is that we're hoping industry will step up to the plate and have Ms. Davidson has talked about, a level of awareness of what information technology is. If not, obviously Congress as a resort could mandate security standards, which we don't want to do.

And with that, I'll adjourn the committee.

[Whereupon, at 2:50 p.m. the subcommittee was adjourned.]