S. HRG. 107–674

HOLES IN THE NET: SECURITY RISKS AND THE E-CONSUMER

HEARING

BEFORE THE

SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JULY 16, 2001

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE
81–757 PDF WASHINGTON : 2004

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii	JOHN MCCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER G. FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*
MARK BUSE, *Republican Staff Director*
JEANNE BUMPUS, *Republican General Counsel*

SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE

RON WYDEN, Oregon, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	GEORGE ALLEN, Virginia
JOHN F. KERRY, Massachusetts	TED STEVENS, Alaska
BYRON L. DORGAN, North Dakota	CONRAD BURNS, Montana
MAX CLELAND, Georgia	TRENT LOTT, Mississippi
JOHN EDWARDS, North Carolina	KAY BAILEY HUTCHISON, Texas
JEAN CARNAHAN, Missouri	SAM BROWNBACK, Kansas
BILL NELSON, Florida	PETER G. FITZGERALD, Illinois

CONTENTS

HOLES IN THE NET: SECURITY RISKS AND THE E-CONSUMER

MONDAY, JULY 16, 2001

U.S. SENATE,
SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 1:05 p.m. in room SR–253, Russell Senate Office Building, Hon. Ron Wyden, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. RON WYDEN, U.S. SENATOR FROM OREGON

Senator WYDEN. The Subcommittee will come to order. I last chaired a congressional subcommittee in the early 1990's, when the Internet was not part of anyone's jurisdiction in the U.S. Congress. Given how dominant the Internet is today in our lives, I think it is appropriate to begin by just looking back for a couple of minutes.

Not very long ago, the Senate Committee on Commerce, Science, and Transportation had a very different purview. Commerce in the United States largely involved the physical movement of goods. This Committee was charged with writing the ground rules for an economy where millions of workers—most of them men, by the way—got up at the crack of dawn, ate thousands of calories for breakfast, and then moved those goods physically from one point to another.

Today, commerce in the United States has changed, and there is an increasing role for the movement of ideas and goods through packets of light. I feel very strongly that it makes no sense to try and shoe-horn the new challenges of a technology-driven economy into rules and policies written for another day. Therefore, a special priority of this Subcommittee will be to examine fresh, creative ideas for a world driven by information technology.

The purpose of today's hearing is to examine how the Internet has changed since its inception, and to look at the security risks and vulnerabilities that have developed along with the rise of e-commerce. All America is reading the newspaper about occasional virus attacks, computer glitches, and hacker mischief, but today this Subcommittee is fortunate to have three excellent witnesses who can look beyond individual incidents and help provide some long-term perspective.

Specifically, we will examine what risks are introduced as Americans move more and more critical business functions onto the Internet, and what can be done to minimize those risks. The Inter-

net is certainly not risk-free, but this Subcommittee will show that there are practical steps the public can take to make the open house of the Internet a safer house and not a house of cards.

Things have changed since the inception of the Net. Worldwide Web has evolved from a platform for researchers sharing information, to an entertaining and useful vehicle for surfing the Web, to a core medium for American commerce. Hacking is no longer a joke, a mischievous prank that teenagers pull for fun. Where e-commerce is concerned, sabotage might be a better term.

As we explore this issue today, there are several elements that I would like to emphasize. First, the Senate should keep its eye on the principal challenge before the Congress, overcoming obstacles to electronic commerce. That is what I have tried to do with the Internet Tax Freedom Act, the Digital Signatures law, and the Y2K liability law. I see reducing risk for the e-consumer as continuing the effort to overcome the obstacles to e-commerce.

Second, the job is not going to get done by taking an ostrich approach to security issues by sticking our heads in the sand and pretending that there are simply no risks. I believe that when consumers and businesses understand fully what those risks are and how to minimize them, they will shift more business functions to the Net, and that is what this Subcommittee hopes to promote.

It is important to do this now, because our lives are increasingly intertwined with the Net. Our mobile phones connect us; our personal digital assistants connect us; and our home appliances may soon be connected to order new groceries or detergent. With this growth, there is going to be an increase in the array of attacks against the Net. Even now, there is something of a sort of hacker hierarchy, allowing two very different kinds of people to damage e-commerce.

Most problems originate with a small minority of people who are certainly not technological simpletons, but their work is now available Internet-wide. Programs today are sophisticated enough to provide a hacking how-to for folks who cannot manage it alone.

There are a number of ways the Government can buttress e-commerce security efforts in the private sector. Law enforcement officials can provide the tools to track down attackers and the consequences that will discourage them. Since people, not programs, will be ultimately responsible for making the Internet more secure, the Government can encourage education and support research and development of security services. The government can also facilitate information-sharing that might not otherwise occur in the private sector, fostering discussions to identify the best practices that might better serve the public Internet-wide.

The New York Times, for example, recently reported that companies providing Internet security are still booming, despite an overall slow-down in the high tech sector. I hope our witnesses today will be able to tell us what risks exist, what precautions we can realistically achieve, and how business and consumers can best meet the security challenges of e-commerce.

We have got a first-rate panel here today. I want to thank all three of you for allowing me, as the new Chairman of this Subcommittee, to begin with such valuable testimony.

Dr. Vinton Cerf is our first witness. He is the Senior Vice President for Internet Architecture and Technology at WorldCom, and is often described as the "father of the Internet." Mr. Harris Miller is President of the Information Technology Association of America, a trade association representing the broad information technology industry.

Finally, Mr. Bruce Schneier is Chief Technology Officer of Counterpane Internet Security, and the author of *Secrets and Lies: Digital Security in a New World.* I want to note for the record, Mr. Schneier comes directly from Las Vegas, where he was at the DEFCON meeting which I saw you described in one of the online services this morning as sort of a cross between a Startrek convention and a Ramones concert.

[Laughter.]

Senator WYDEN. I thought that was certainly an apt and colorful way to describe it.

Gentlemen, we welcome all of you. We are going to make your prepared remarks a part of the record in their entirety. Dr. Cerf, why don't you begin.

STATEMENT OF DR. VINTON G. CERF, SENIOR VICE PRESIDENT, INTERNET ARCHITECTURE & TECHNOLOGY, WORLDCOM

Dr. CERF. Thank you very much, Mr. Chairman, and may I say that that was a remarkable summary of the problem at hand in such a short period of time. Plainly, you have taken the reins of this Subcommittee and you are on your way.

I would like to first thank you for inviting me to participate in these hearings today. I think it would be helpful to begin by reminding everyone that the Internet's origins now nearly 30 years ago were academic and research-oriented in nature. Although the work was funded by the Defense Department, almost all the work actually went on in an academic setting.

The network itself was not for commercial use at all until about 1990. Now, I have to say with some mixed feeling that in fact there was a DARPA-sponsored classified design for a fully secured network for military use that was begun in 1975, and that was a classified effort, and I was never allowed to release any of the results of that work to the academics who were participating in the public version of the Internet, so today we find ourselves struggling with some network security problems that might have been solved a few decades ago, if only we could have released the information. Plainly, at the time, that would have been inappropriate, so we just have to deal with the alligator that faces us now.

Commercialization of the Net did not happen until 1989, when the Federal Government gave permission for the use of the NSF Net backbone for commercial activity, and released, or at least made less restricted the appropriate use policies for that system. That quickly led to commercial Internet services in the form of Internet service providers, one of which is UUNet, which is a company now integrated into WorldCom. The other is PSINet. Those were the two first commercial services in the United States.

The worldwide Web arrives technically in 1989, but visibly only in 1994, and it shows up in the public view in the form of Netscape

Communications, and then later, of course, software from Microsoft and others, so the general public did not see Internet as part of its visible universe until 1994, which is now only 7 years ago.

The intensity of commercial use has been rising since that time, and in particular, many, many of the commercial applications arose in the context of the worldwide Web. Today's network has about 500 million users. That is a small number relative to the world's population of 6 billion, but it is still a fairly large population of users.

There are about 150 million computers on the Net acting as servers, and an additional 300 million or so personal computers or other Internet-enabled devices, personal digital assistants, and now even cell phones, so it is a fairly large universe of users and servers in the system.

For purposes of this discussion, I would like to split the Net into three parts, a backbone, a host component, and a client component. The backbone is the system that the Internet service providers operate. It is the communications portion of the Net. The hosts are the things that supply services. That is where the applications run, and the clients are the personal computers, personal digital assistants and the like, that the users operate.

The risks of using the Net fall into those three different categories. I would also note that in spite of any deliberate attacks and others things, that Murphy's Law is still very much at work. We are all capable of shooting ourselves in the foot, and we seem to do it regularly, without the help of hackers.

Let us talk about backbone threats. One of the most visible is what is called the denial of services threat. It is something that simply overwhelms the target with too much traffic. There is a particularly fancy version of it called distributed denial of service attack, which means that the attackers are scattered over hundreds of thousands of machines, and it is very hard to isolate any one of them as the source of the attack.

There are also attacks—those, by the way, are launched typically against the host computers. There are also attacks against the core of the Net, the routers and the other elements that actually move packets back and forth, so that the Internet service providers have to protect against that by one means or another.

Threats against the host and the Net often go against the operating system vulnerabilities. The operating system of a machine, or of a Web server, is what essentially keeps it running, but there are all kinds of attacks that are possible, because there are all of these bugs in the software that create vulnerabilities and, of course, smart people find them.

There are even attacks against passwords. Unfortunately, we use what are called reusable passwords to a greater degree than we should. That means that it is the same password. Every time you put a user name in, you put a password in, and since it is the same one every time, it is often possible to mount what are called dictionary attacks against people's passwords, even if they are encrypted by what is called a one-way encryption function, and kept on the host computer.

It is possible to encrypt all the words in the dictionary and compare, if you get your hands on it, with the one-way encrypted pass-

word files, and if you find a match, then you just check to see which word in the dictionary that matched, and that might be the password, so unfortunately, reusable passwords are a bad habit.

To make things worse, people pick really bad passwords. They pick their birth dates, and their wives' mothers' names, or their past names, things like that, things that other people might know, and might be able to guess, so we have some training to do of users.

Then there are Trojan horses. These are pieces of software that can be injected into a host computer or another computer and run in the background to do bad things to you later on.

Probably the most visible threats, though, that show up are threats against personal computers themselves. These are software attacks, and you hear words like viruses, and worms, and things of that sort. These are codes that are carried into your computer, sometimes by electronic mail attachments, and they do all kinds of damage, the I love you virus being one of the most visible, and possibly one of the most expensive ones.

We are faced with more risks as we put more and more people on line on a permanent basis. Instead of dialing into the network, which is what 80 percent of the users do today, people get on the Net on a permanent basis with digital subscriber loop technology, or cable modems, but that means their machines are exposed 24 hours a day while they are online, and most of the personal computers of the world were not designed to withstand the sorts of attacks that can be mounted against permanent hosts on the network, and so that is yet another source of vulnerability.

There are other risks that consumers face, and I am just going to mention a few, because I am now over time, and I appreciate the Chairman's indulgence.

Senator WYDEN. Go right ahead.

Dr. CERF. Some people imagine that e-mail is private, and that once you have thrown it away it will not ever appear again. Well, it turns out that in order to provide good-quality service, often the e-mail service providers back things up for you.

I had a little incident a few months ago where some messages from two years ago were sitting in an old computer that woke up one day and realized that none of those messages which had been stored away as a backup had been delivered, and it panicked about this, and sent notes out to everyone who sent those messages to me saying this message has not been delivered in two years, there must be something wrong, and of course I got an avalanche of messages from my friends saying, I am getting messages I sent to you two years ago back from this machine, and why are you doing this.

Of course, I had no idea what was going on, so if anyone believes that e-mail is private, please take note, it may not be.

There are other risks. Identity theft is common and increasing, and the network is used in part of that. Credit card theft, even fraudulent storefronts that put up what look to be businesses, but are simply in the business of capturing your credit card for purposes of abusing it later.

What about public access to Government records? Is that a risk? Well, it could be, if lots of details about your house and the design of it and all the other details that may be your transactions with

the system of justice, all of which are public records, but in the past they have not been easily obtained, and now they are online, and that could be an issue.

And then there is cyber-stalking, just to name another thing, where people are tracked through the network e-mail is sent to them, harassing them.

Other kinds of activities could potentially be conducted through the network, and constitute yet another consumer risk. You are going to hear from my colleagues in a moment. Bruce is going to tell you that eternal vigilance is the price of security on the Net. You cannot secure the network once and have it be locked up. You have to keep checking over and over again to make sure it is still buttoned up, and what Mr. Miller is going to tell us among other things is that industry cooperation is critical for network security to be achieved by the industry. We cannot do this each individually by ourselves.

And of course, Mr. Chairman, you are wondering what on earth can the Congress do about this. Well, one thing that you should not do is pass legislation that cannot be enforced, and so if it is technically impossible to enforce a piece of legislation, it leads to all kinds of side-effects, one of which is people ignore the law, and I think ignoring the law is a very bad precedent to set, so one wants legislation which is enforceable.

Possibly the most valuable things you can do in the near term would be to pass laws, if necessary, to help us prosecute offenders to make sure that those who are apprehended and do such damage can, in fact, be successfully prosecuted and punished.

There is a balance here which I think is difficult for you, and that is to figure out how to create those laws, while at the same time protecting the rights of personal privacy, and that balance is not easy. One could imagine building a very secure network environment by simply observing everything everyone does, and anything that looks even the slightest bit improper could be captured, recorded, and analyzed.

I would not be a strong proponent of such an approach, but it is plain that that balancing act lies squarely in the hands of the members of this Subcommittee and the Members of Congress.

Well, let me stop there, Mr. Chairman. I appreciate your allowing me to go on at length. I think you will find the comments of my colleagues to be most enlightening.

[The prepared statement of Dr. Cerf follows:]

PREPARED STATEMENT OF DR. VINTON G. CERF, SENIOR VICE PRESIDENT, INTERNET ARCHITECTURE & TECHNOLOGY, WORLDCOM

Introduction

As a historical matter, the Internet and its predecessor systems were developed in a largely academic environment focused on research, information and resource sharing and a general atmosphere of cooperative enterprise. For over twenty years, from 1969 to 1990, the Internet research program and user population benefited from this academic setting. However, by 1990, the environment began to change. For one thing, Internet services were just beginning to be made available on a commercial basis. As the cross section of users changed from its academic and military origins to encompass the business sector and the general public, a far broader range of behaviors were manifest in the Internet world. Various kinds of vandalism and other deliberate attacks increased in incidence.

If not daily, then more often than one would like, one reads reports about a variety of network vulnerabilities, hacker attacks, unintended information releases and other frailties on the Internet. For the most part, these problems center on the computers that serve users on the Internet, but a good number also reflect vulnerabilities of the network itself. The network vulnerabilities are a primary concern for the Internet Service Providers who have responsibility for keeping the Internet in operation 24 hours per day, 365 days per year. It is also worth observing that many of the operational problems arising on the Internet have little to do with deliberate attacks. Rather, these problems arise simply from the complexity of the system, the proclivity of Murphy's Law to take effect at any moment,[1] bugs in the software, human errors and things that simply break down. While network-related problems are a consumer concern, to the extent that they interfere with access and use of Internet services, the more critical concerns revolve around the serving computers (so-called Internet hosts) through which all online services are implemented, the client computers (desktops, lap-tops, personal digital assistants, internet-enabled cellular phones, and so on) and the policies of companies that provide services through the Internet. I will concentrate my testimony, therefore, on the end-points of the Internet: hosts, client devices and the companies that provide Internet-based services.

Consumers are particularly vulnerable to weaknesses in application software. Email can carry attachments that harbor so-called "viruses" that can "infect" the rest of the software in the user's computer. Web pages can deliver software that is interpreted by the user's browser and may cause damage to the user's information or interfere with proper operation of the user's computer. This topic is explored in more detail later in this paper.

Host Vulnerabilities

Among the most visible of the consumer-affecting problems are denial-of-service attacks aimed at interfering with the normal operation of one or more servers on the Net. These attacks are sometimes very hard to distinguish from legitimate overloads, such as the famous Victoria's Secret Lingerie webcast that drew a reported 1.5 million viewers whose attempts to download streaming video completely outstripped the server's ability to deliver traffic. The server simply could not respond to all the user requests for data. Such problems are analogous to overloaded emergency service centers that cannot accept all the telephone calls made during a crisis.

If the overload comes from a single source or a small number of sources, ISPs sometimes can track down the source and filter out the offending packets as they enter the network. However, hackers have developed distributed denial-of-service (DDOS) attack tools that harness tens to hundreds of thousands of computers in the Internet. Each of these may send only a small amount of traffic but the aggregate may overwhelm the target. Such attacks are much harder to defend against and to track down. A principal reason that such distributed attacks are even possible is that many hosts on the Internet are unprotected from break-ins and become unwitting "hosts" for so-called "Trojan horse" software that can be activated remotely and used to originate traffic towards the target. The irony of this situation is that the unprotected hosts often contain no information or provide no services that are considered critical in nature. They might be serving computers and workstations in an academic setting. They might even be laptops or desktops that are connected to the Internet by dedicated links (such as Digital Subscriber Loops or cable modems). If these platforms can be found by methodical probing of the Net, they may be subsequently "infected" with "zombie" software that can later be used in a DDOS attack. But because these computers might not be thought to contain critical or valuable information, they may not be as protected from invasion as they might otherwise be.

These vulnerable resources may not be configured by their operators to be resistant to the exploitation of vulnerabilities. The systems may be operating with "default" passwords that come with the manufacturer's "standard" configuration—such passwords are widely known (especially among the hacking crowd) and should be changed by the operator before going online. Desktop machines (and operating systems) that were designed to be used mostly as client computers, may become more vulnerable when they participate in so-called "peer-to-peer" operations. Examples of such applications include Instant Messaging, file transfer services, Internet telephony and so on, in which the computer behaves both as a client and as a server.

Apart from a variety of denial-of-service risks associated with host machines on the Net, e-consumers run a variety of risks of information compromise in which data

[1] Murphy's Law reads, "If anything can possibly go wrong, it will." A corollary suggests that Murphy was an optimist!

they consider private could be exposed to unauthorized view. The least technical and most common avenue for such exposure is a consequence of corporate policies that simply do not protect consumer privacy. User names, addresses, telephone and fax numbers, email identifiers, account numbers, social security numbers, credit card numbers and any of a variety of other data might well be released, deliberately, by a corporation that does not have a consumer privacy protection practice and chooses to share this information for business purposes. The same data might be released unintentionally by the operator of a host who has failed to protect an online system from exploitation.

One of the more ironic scenarios occurs when the user's client computer establishes an encrypted channel over the Internet to a server machine, transmits private information to that machine, and the information, so carefully protected while in transit, is exposed to unauthorized parties either by business practice or by negligence in configuring the server from invasive attack.

Rip Van Wrinkle

Consumers are sometimes surprised by the unexpected consequences of well-intended service features. For example, a few months ago, I suddenly received a barrage of messages from my email correspondents who reported that a batch of messages they had sent me nearly two years ago had suddenly emerged on the Internet accompanied by rejection notices saying that these messages had not been delivered. A back-up email server had received and recorded these messages and awakened from its slumbers (for reasons never quite clear) to realize that from its perspective, this cache of messages had not been delivered in two years. The machine dutifully set out to notify every sender of this fact and included a copy of the "undelivered" message.

More generally, email services often make backup copies of the email so as to recover from a catastrophic failure of a primary server. From time to time, email users are surprised to discover that email they thought they had long since deleted has been retained in backup files and has been released by accident or has become discoverable in a legal proceeding or is accessible under appropriate warrants. This is perhaps a specific case of the more general case of record keeping, such as is done in the consumer telecommunications service industry. Detailed billing records of calls (telephone number called, originating telephone number, date and time of day of call) are often kept for periods ranging from three months to a year to resolve subsequent disputes. Anyone who uses a major credit card that provides a report annually on their use can confirm that the credit card industry knows a great deal about specific consumer activities in the form of detailed transaction records.

Passwords

One of the more serious consumer risks arises in the use of access-controlled services requiring user authentication. The most common method of authentication is to associate a "password" with a user identifier (ID). These passwords are often fixed and reused repeatedly. Users are notorious for the poor choices of passwords and their unwillingness to change them regularly. Passwords can often be guessed (birthdate, pet's name, spouse's name, the current year, anniversary date, social security number, telephone number, address). Password files at the service hosts are usually one-way encrypted[2] but if a hacker can get a copy of the encrypted password file it is possible to run a "reverse dictionary attack" to try to find the password. In a reverse dictionary attack, all the words in the dictionary are encrypted and then compared with each of the encrypted passwords taken from the target computer. A match exposes the password. Such tools are very commonly available. Good password practices dictate at the least that reusable passwords be changed regularly, contain more than just alphabetic characters, be 6–10 characters long and not contain common words found in the dictionary. An example of such a password is "SOLIPIKU98."

There are a number of alternatives to these so-called "reusable" passwords. Some of these require the use of a device that introduces a constantly changing password. Others authenticate by means of a challenge and an encrypted response that can be verified.

Risks

The July 2, 2001 edition of TIME Magazine carried a cover story devoted to online privacy risks faced by consumers. Identity theft is one of the most critical and in-

[2] "One-way" means that the original password is encrypted in such a way that even if you know the encryption algorithm, you cannot directly decrypt the password. However, one could use a dictionary, encrypt its words, then look for encrypted text in the dictionary that matches the one-way encrypted password.

creasing risks faced by consumers. Information about consumer use of Web services can be collected in each user's personal computer by Web service providers in small caches of information called "cookies." The Web service providers can use this information to tailor services provided to individual users. However, this data might contain personal information that could be linked with data obtained through other sources and possibly even re-sold to third parties for marketing purposes. Consumers are at risk if companies that collect this data make use of it in ways that consumers do not expect or would not approve. It is this concern that led to requirements for companies to report their privacy protection practices to consumers on a regular basis.

Not all Web sites are what they seem and some may appear to offer products or services but may in fact simply be "fronts" for purposes of capturing personal information, credit card numbers and the like. This is outright fraud. It is illegal and actionable.

Public access to government records may expose a considerable amount of personal information to public view. Details of court records, registrations, building permits and designs, home addresses and phone numbers, traffic violations are all potentially available. This is through no weakness in the design of the Internet and its applications but a consequence of state or local policy with regard to access to "public" records.

So-called "data brokers" obtain personal information from a variety of sources, often government sources, and amass databases of personal information which they then resell to the public for a fee. There is often considerable debate about the legality of making such information accessible, even if it is obtained by legitimate means from legal sources.

Software can be put into your computer by someone with physical access to it that will provide a record of virtually everything you do with your machine. Similar software might be ingested over the Internet as an attachment to an email message or possibly as a consequence of loading a Web page and executing "applets" (written in programming languages such as Java). Such "Trojan horse" software can expose all of your personal computer's data and activity to view. The recent wave of interest in dedicated, high speed access to Internet using Digital Subscriber Loops (DSL) or cable modems creates a new risk for consumers. If their computers are online all the time, with fixed Internet addresses, they may become subject to hacker attacks, just as the Web servers and other Internet hosts are exposed today.

Consumers may be misled by email, chat room or instant messaging exchanges into believing things about their correspondents that are not true. This works both ways. A person may misrepresent himself or herself deliberately or you may be the target of an attack against you by someone pretending to be you. Such terms as "cyberstalking" have entered the language to account for this kind of behavior.

Reactions

Consumers can respond by being far more careful about the information they provide to online service providers. They can avoid downloading, opening or executing attachments on email messages until they confirm their origin. They can purchase, use and frequently update virus detection software. Even if you use secure Web sites, the protection extends only to the delivery of personal information to the Web site. The Web service provider's privacy protection policies determine whether the data provided is propagated further to third parties. Consumers should make a point of learning company privacy protection policies.

Companies seeking to protect their own computing assets and networks can install firewalls and make use of encryption methods to protect employee access to corporate networks via the public Internet. Software manufacturers need to pay closer attention to the potential abuses their software can support—not simply focus on the constructive functionality they offer. Internet service providers need to configure their networks to increase resistance to various forms of hacking. And legislators may be able to help law enforcement agencies by providing tools for combating criminal use of online systems. There is a tension in the latter response because it is possible to erode privacy in severe ways in the process of trying to assist in law enforcement.

The Internet has the potential to be an enormously powerful, positive and constructive force in our society. It is also a potential source of serious abuse. As a society, we are challenged to find a balance between protecting the society from abusive practices and protecting individuals from abuse by various state, local and federal government agencies. The next decade will surely be filled with unexpected twists and turns as we learn how to apply online technologies to our daily needs. One can only hope that out of all the experience will come wisdom and the will to apply it.

Senator WYDEN. Dr. Cerf, thank you for an excellent statement, and your admonition to pass no foolish laws; that is particularly important. Congress has to look at these issues in a different way.

The Internet is this vast system, decentralized, made up of millions of content-creators worldwide, and the last thing that one should do would be to impose a sort of Washington one-size-fits-all solution. That, as you say, would just breed contempt for the law because it could not be enforced. Your points are very well-taken. I will have some questions in a moment, and feel free, any time I am around, to go over the time limit, because that was very well-said.

Dr. CERF. Thank you very much.

Senator WYDEN. Mr. Miller, welcome.

STATEMENT OF HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. It is good to see you again, Mr. Chairman. Thanks for including ITAA in this hearing. In our 40th anniversary year, we have spent a lot of time focusing on the issue of cyber security, and one of the obvious reasons is that because so much of the Internet as Dr. Cerf has described it is managed, owned, and operated by the private sector.

In fighting physical crime, we always look to Government as the lead, because Government has the law enforcement tools and the law enforcement community to do that. However, in fighting cyber crime, there is a unique onus on the private sector in partnership with Government to come up with solutions.

Certainly, one thing which we believe is particularly important, Mr. Chairman, is a higher level commitment both in corporations and in the Government to fighting cyber crime. That is because consumers demand it, and citizens demand it. As Dr. Cerf pointed out, the Internet has morphed into something now where the commercial and governmental reliance on it is very high, and yet the focus on security has not been, up until recent years, a major part of the Internet, but even with this growth, as Dr. Cerf pointed out, the Internet is still in its infancy.

At any one time, no more than 3 or 4 percent of the globe is connected to it, and most experts will tell you that in the not-too-distant future we will live in a truly digital world transformed by Internet technology.

The Internet today, which we think of as basically a PC-based model sitting at our desk, will change dramatically to become ubiquitous, seamless, and integrated into everything we do. Digital ubiquity means that we no longer will think about how we use and access information on the Internet. A virtual information bubble will be formed around our lives, anticipating and addressing many of our needs, and this mobile commerce, sometimes called m-commerce, or ubiquitous commerce, called u-commerce, will be enabled by wireless networking.

Now, how important is this wireless issue? Well, I understand, Mr. Chairman, that there is a major United States Cabinet official who has been prohibited by his staff from using his wireless PDA because of concern about security, and I suggest that this kind of attitude toward the wireless Internet is not the way we move to-

ward ubiquity. The security challenges in the wire-line world, as extensive as they are today, will become even more extensive in the wireless world.

Let us put this concept into perspective. In the world today there are about 20 billion microprocessors, give or take a few. Only about 3 billion of them, however, are in computers. These others are going to be linked going well beyond some of the devices we think about today, such as the cellular phone which I have with me, or my PDA, into all kinds of aspects of our lives, into automobiles, into thermostats in your homes, smart tags used for tollways, and all kinds of other opportunities which we are just beginning to think about.

Operating on multiple protocols, which is part of this development of the wireless world, magnifies security vulnerabilities, and this proliferation of devices and protocols is not surprising, because we are still in the early days of this ubiquitous Internet, but we need to develop viable security solutions not just in the wire-line world, but also in the wireless world.

Again, we must have this high-level commitment from the CEO's, from boardrooms, by political leaders at all levels of Government, and this attention must be global, not just in the U.S., because we are talking about a global medium.

We must bring together vertical industries, which are unfortunately sometimes segregated, such as telecommunications, IT industry, health care, finance, energy, and others, and create a broad industry dialog on additional pieces to the security puzzle which will take us toward this ubiquitous Internet. We need to move toward consolidation, toward simplification, toward improved security, if we are going to have a truly ubiquitous Internet.

Today, I suggest a four-point call to action for industry to focus beyond the security realities of today by addressing u-commerce. First, we need industry collaboration at the highest levels. Simply bringing together technical people, as important as they are, will not get the job done.

Second, this collaboration must be across industries. Again, the Internet industry itself cannot solve all these challenges.

Third, we have to put aside some egos and some initial investments and come together for consolidation and collaboration, and it must focus on a point which I know is very dear to your heart, Mr. Chairman, that privacy and security are often two sides of the same coin.

We at ITAA are already starting to address this challenge, which we know will not be easy to meet. No one, least of all the IT industry which I represent, wants to be dictated to about its products and capabilities. After all, the IT industry believes it knows best its own industry. But I believe unless we get some common threads going on these issues, it will be very difficult to get a secure world in a wireless Internet.

A couple more points about cyber security, which I know Mr. Schneier will also be addressing. Too often, the assumption is made that improving cyber security and fighting cyber crime can be done with technology alone. Just give me the right software, just give me the right hardware, just give me the right firewall and I am all set.

That is wrong. Just as the best alarm system will not protect a building if the alarm code falls into the wrong hands, or is not turned on at night, a network will not be protected if the passwords are given out freely. Failures in the people and in the processes part of the cyber crime solution may, in fact, be the majority of the problems we see.

That means that organizations must be willing to invest not just in the technology solutions, but also in the training, the security procedures, and this must be across the enterprise, not just in the IT department. We need to practice what Dr. Cerf has called cyber hygiene. Everyone needs to be a part of the solution.

Now, in many ways, solutions of cyber security challenges are no different than any other Internet-related policy issue. Industry leadership, again, must be the hallmark—but, Government does have an important role.

So let me review a few points that I believe Government must focus on. First, I would like to reiterate the point Dr. Cerf made. The Congress must provide for what I call the Internet Hippocratic oath. First, do no harm. Do not try to pass laws that seem to be ways of dealing with the challenge, but in fact miss the mark.

Second, Government must do a better job of practicing what it preaches. The rules of the challenges of technology, people, and processes apply to the Government sector just as much to the private sector, yet we constantly hear about failures in the Government. The U.S. Government must lead by example in preventing intrusions into agency Web sites, data banks, and information systems. Leadership in this area means substantial investments, which I fear candidly are not being made today, Mr. Chairman, to deal with the cyber security challenge to the Government.

Number 3, we need a more sophisticated process in the Government of leadership. ITAA has advocated the creation of an information security czar similar to the one that John Koskanen played as the Y2K czar. We have been told that is not likely to happen, but we have also been advised of a draft executive order which may be issued soon by the President which will bring more centralization and focus to Government leadership, and we believe that is absolutely essential, and look forward to the issuance of that executive order, leading to more coordination across all agencies of Government, not just law enforcement and national security.

Funding. Funding is critical. Funding is critical in terms of IT spending for the Government, in terms of research and development, in terms of work force. We need to focus on these issues, not to waste money, not to duplicate what the private sector is doing, but to coordinate and collaborate with the private sector.

In conclusion, Mr. Chairman, society's reliance on the Internet has just begun. The ubiquitous Internet, u-commerce, is going to mean more people connected to the Internet, and they need to also have the trust and confidence that these media they are using are reliable, so it is important that we focus, as this Subcommittee is doing, on information security, and come together to meet the challenges.

Thank you very much.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Introduction

Chairman Wyden and Members of the Subcommittee, thank you for inviting me here to testify today on Internet security. My name is Harris N. Miller, and I am President of the *Information Technology Association of America* (ITAA), now celebrating its 40th Anniversary. I am proud that ITAA has emerged as the leading association on cyber security issues. ITAA represents over 500 corporate members. These are companies that have a vested economic interest in assuring that the public feels safe in cyberspace; in the United States and around the world, the vast majority of the Internet related infrastructure is owned and operated by the private sector.

I am also President of the *World Information Technology and Services Alliance* (WITSA), a consortium of 41 global IT associations from economies around the world, so I offer a global perspective. ITAA also houses the *Global Internet Project* (GIP), an international group of senior executives that are committed to fostering continued growth of the Internet, and which is spearheading an effort to engage the private sector and governments globally on the Next Generation Internet and related security and reliability issues. The GIP recently sponsored a major event on security and privacy in the next generation of the Internet that drew industry leaders from around the world.

I commend this Subcommittee for holding today's hearing on Internet security, and I submit to you that security is ultimately a business challenge that must be addressed at the highest levels of corporate hierarchy. Customers and citizens—whether consumers in the B2C space, or business partners in B2B operations, or Americans receiving services electronically from their governments—demand it.

The stakes involved are enormous. Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, and over 8 percent of US GDP, according to *Digital Planet 2000,* a report released last year by WITSA. According to the *US Department of Commerce,* IT accounted for approximately one-third of the nation's real economic growth from 1995 to 1999. Despite the current slowdown, IT-driven productivity increases have enabled our country to have what many economists thought we could not have: high growth, low unemployment, low inflation, and growth in real wages.

The IT industry's importance to the economy goes beyond the numbers I just recited, however, because the IT industry is not only a vertical industry—such as financial services or health care—it is also a horizontal industry whose technology and services under gird all the other industry sectors. For instance, the failure of a particular IT company to meet the information security challenge not only hurts that company's bottom line, it also hurts the bottom line of companies to which it provides software or IT services.

The Evolution of the Internet

In order to look at security issues surrounding the Internet, we need to first recall its intended nature. The Internet, when it was created nearly thirty years ago, was a collaborative product developed by industry, government and academia. It was designed to be an open, borderless medium for communication and sharing information, and was not programmed with security features. Nor was it intended for commercial use.

As they say, we've come a long way, baby. As you know, the Internet today is used extensively as a commercial medium, augmenting or even forming the basis of entire business models. Forrester research estimates that worldwide B-to-C e-Commerce revenues will reach $96 billion this year. According to a report by eMarketer, B-to-B online commerce revenues will nearly double this year to reach $448 billion, with fifty-seven percent of that commercial activity occurring here in the U.S.

And we are moving forward still. Quickly. Most Internet executives will tell you that in the not too distant future, we will live in a truly digital world, transformed by Internet technology. The Internet will be ubiquitous, seamless and integrated into everything we do. Digital ubiquity means that we no longer consciously think about how we use and access information on the Internet. Phrases like "always on" and "24/7" will be quaint. Just as we assume that the power grid is always available, we will have Internet Protocol in and on everything—our cars, our home appliances, even the products we buy at the supermarket. The Internet will allow these items to communicate—forming a virtual information bubble around our lives, anticipating and addressing many of our needs.

Mobile or Ubiquitous Commerce will be enabled by wireless networking. Individuals will move from network to network through the use of mobile computing, becoming guests on others' networks. This is already starting to happen around the globe.

The growing e-commerce space and the very real prospect of digital ubiquity pose challenges in securing the Internet. Government and businesses increasingly have as much at stake digitally as physically. Assets and value are no longer based on material objects but on information, knowledge and network connections. In the old economy and the new, more businesses are using technology to manage operations, sales, employee relations, partnerships and supply chains. More revenue is derived and more cost savings realized from online activity.

Yet the same companies and organizations that devote considerable financial and human resources to physical security pay much less attention—or, sometimes, virtually no attention—to cybersecurity. Just like a business cannot properly function without sound financial processes and systems, the same has become true for managing network activity and the valuable, critical information that flows through the network.

As I mentioned earlier, the Internet was not designed with commercial and security features in mind, yet as businesses become dependent on it for growth and market share, vast security needs have emerged. ITAA believes strongly that for this reason, Internet security measures must be addressed at the CEO and boardroom level of every company and by political leadership at all levels. And this attention must occur around the globe, not just in the U.S.

Economy at Risk

Cyber crime places the digital economy at risk. Just as the reality or threat of real crime can drain the economic vitality of neighborhoods, cities and even nations, so to can the reality or threat of crimes committed online against people and property shutter businesses and cause an otherwise motivated digital public to break their Internet connection.

Cyber crime falls into several categories. Most incidents are intended to disrupt or annoy computer users in some fashion. Distributed denial of service (DoS) attacks crash servers and bring down websites through the concerted targeting of thousands of email messages to specific electronic mailboxes. Viruses and other malicious code introduce phantom computer software programs to computers, designed intentionally to corrupt files and data. Other online intrusions are conducted to deface websites, post political messages or taunt particular groups or institutions. Even though no one stands to profit, damages caused by such attacks can run from the trifling to the millions of dollars. What motivates these attackers? Hackers may view the attack as a technology challenge, may be seeking to strike a blow against the establishment, may be looking for group acceptance from fellow hackers, or may be just indulging themselves in a perverse thrill.

Other cyber criminals are more material guys and gals. They hope to profit from their intrusions by stealing valuable or sensitive information, including credit card numbers, social security numbers, even entire identities. Targets of opportunity also include trade secrets and proprietary information, medical records, and financial transactions.

For some cyber criminals, the Internet is a channel for the dissemination of child pornography and a tool used in the furtherance of other crimes against children and adults. These crimes include fraud, racketeering, gambling, drug trafficking, money laundering, child molesting, kidnapping and more.

Cyber terrorists may seek to use the Internet as a means of attacking elements of the physical infrastructure, like power stations or airports. As we have seen in the Middle East, cyber terrorists encouraging political strife and national conflict can quickly turn the Internet into a tool to set one group against another and to disrupt society generally.

Another class of cyber criminal and, unfortunately, the most common is the insider who breaks into systems to eavesdrop, to tamper, perhaps even to hijack corporate IT assets for personal use. These could be employees seeking revenge for perceived workplace slights, stalking fellow employees, looking for the esteem of peers by unauthorized "testing" of corporate security, or other misguided individuals.

Regardless of category, the threat is real. *A recent study* produced by Asta Networks and the University of California San Diego monitored a tiny fraction of the addressable Internet space and found almost 13,000 DoS attacks launched against over 5000 targets in just one week. While most targets were attacked only a few times, some were victimized 60 or more times during the test period. For many small companies, being knocked off the Internet for a week means being knocked out of business for good.

The Computer Security Institute/FBI also documents the problem in a widely reported study on computer breaches. This year's survey of 538 respondents found 85 percent experiencing computer intrusions, with 64 percent serious enough to cause financial losses. Estimated losses from those willing to provide the information tallied $378 million, a 43 percent increase from the previous year.

A nationwide public opinion poll released last year by ITAA and EDS showed that an overwhelming majority of Americans, 67 percent, feel threatened by or are concerned about cyber crime. In addition, 62 percent believe that not enough is being done to protect Internet consumers against cyber crime. Roughly the same number, 61 percent, say they are less likely to do business on the Internet as a result of cyber crime, while 33 percent say crime has no effect on their e-commerce activities. The poll of 1,000 Americans also revealed that 65 percent believe online criminals have less of a chance of being caught than criminals in the real world, while only 17 percent believe cyber criminals have a greater chance of being caught.

These threats collectively represent a chipping away at the trust that is so critical to the Internet. Thankfully, technology is moving faster than public policy ever could to secure the technology that will dominate our economic future.

The Industry Securing the Internet: Information Security

Information security, or cyber security, is the multifaceted discipline that counteracts cyber crime and works to secure the Internet. Information security—or InfoSec—deals with cyber crime prevention, detection and investigation. How do we achieve improved security for the Internet of today and minimize the security challenges of tomorrow's Internet?

Cyber Security is Built From Technology, Processes and People

Too many times, the assumption is made that improving cyber security and fighting cyber crime can be done with technology alone. That is wrong. Just as the best alarm system will not protect a building if the alarm code falls into the wrong hands, a network will not be protected if the passwords are given out freely. Failures in the "process and people" part of the cyber crime solution may, in fact, be the majority of the problems we see. Processes and people tend to be the more problematic elements of the Internet security puzzle. The two are closely linked. From a strategic point of view, the challenge is to make cyber security a top priority issue. Moving from platitudes to practical action requires the sustained commitment of senior management.

The goal is to embed cyber security in the corporate culture. That is not always easy to do. CEO's want their IT systems to be as fast as Ferrari but as safe as an armored truck. Whenever tradeoffs arise, the bias is towards speed, not safety and security. The challenge for the IT sector and its customers working together is to provide security at the speed of business.

Organizations must be willing to invest in the development of comprehensive security procedures and to educate all employees—continuously. We call this practicing sensible cyber hygiene, a term that my friend Vint Cerf frequently uses as he speaks about these challenges around the globe. The primary focus of improving processes and changing behaviors is inside the enterprise. However, the scope of the effort must also take into account the extended organization—supply chain partners, subcontractors, customers, and others that must interact on a routine basis.

With cyber hygiene practices in place, companies can more effectively use the technologies that are available. A very simple example is that a company may diligently employ the latest virus detection software. But, if individual users within the company do not regularly heed messages to update virus profiles covered by the software, it renders the company's security less effective.

Industry Plan for Cyber Security

ITAA and its members have been working to execute a multi-faceted plan designed to improve U.S. cooperation on issues of information security. However, Mr. Chairman, we would all be remiss if we believed it was just the IT industry that must cooperate within its own industry—we must work cross industry, and industry with government. Protecting our infrastructure is a collective responsibility, not just the IT community's role.

We are working on multiple fronts to improve the current mechanisms for combating threats and responding to attacks through our role as a Sector Coordinator for the Information and Communications sector, appointed by the U.S. Department of Commerce. Through ITAA's InfoSec Committee, our member companies also are exploring joint research and development activities, international issues, and security workforce needs. Elements of the plan include Information Sharing, Awareness, Education, Training, Best Practices, Research and Development, and International Coordination.

Information Sharing: Sharing information about corporate information security practices is inherently difficult. Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments. Nor would they risk voluntarily opening themselves up to bogus but costly and time-consuming litigation. Releasing information about security breaches or vulnerabilities in their systems presents just such risks. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor—or worse—consumer confidence in a company's products. Companies also fear revealing trade secrets to competitors, and are understandably reluctant to share such proprietary information. They also fear sharing this information, particularly with government, may lead to increased regulation of the industry or of electronic commerce in general.

Public policy factors also act as barriers to industry information sharing. One of the obstacles is the Freedom of Information Act (FOIA). Companies worry that if information sharing with government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing or costly. FOIA requests place the private sector's requirement for confidentiality at odds with the public sector's desire for sunshine in government information. We are working with Congressman Tom Davis (R-VA), Senator Robert Bennett (R-UT), and other key players on legislation to meet this concern.

Anti-trust concerns are a second potential legal hurdle to information sharing. Fortunately, such risks appear small. The antitrust laws focus on sharing information concerning commercial activities. Information Sharing Advisory Centers (ISACs) should be in compliance with the antitrust laws because they are not intended to restrain trade by restricting output, increasing prices, or otherwise inhibiting competition, on which the antitrust laws generally focus. Rather, ISACs facilitate sharing of information relating to members' efforts to enhance and to protect the security of the cyber infrastructure, so the antitrust risk of such exchange is minimal. The Justice Department has also indicated that there are minimal antitrust concerns involving properly structured joint industry projects for dealing with externalities. An entity created to share information regarding common threats to critical infrastructure should fall into this category.

Given the changing nature of the cyber crime threat and in spite of the many business, operational and policy hurdles standing in the way, many companies in the private sector recognize the need to have formal and informal information sharing mechanisms. Internet Service Providers are an example of the latter circumstance. Because these firms provide networking capability commercially, these businesses often have extensive network security expertise. Such firms act as virtual Information Sharing and Analysis Centers, gathering information about detected threats and incursions, sanitizing it by removing customer specific data, and sharing it with customers.

The IT industry has adopted a formal approach to the information sharing challenge. In January 2001, nineteen of the nation's leading high tech companies announced the formation of a new Information Technology Information Sharing and Analysis Center (IT–ISAC) to cooperate on cyber security issues. The objective of the IT–ISAC is to enhance the availability, confidentiality, and integrity of networked information systems. The group has made excellent progress in the six months since its founding and is in the process of being formally "stood up," although information sharing is already beginning to take place within this ISAC.

The IT–ISAC is a not-for-profit corporation that will allow the information technology industry to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures. Its internal processes will permit information to be shared anonymously. The organization is a voluntary, industry-led initiative with the goal of responding to broad-based security threats and reducing the impact of major incidents. Membership in the IT–ISAC is open to all U.S.-based information technology companies. It will offer a 24-by-7 network, notifying members of threats and vulnerabilities. The group also is clear on what is will not undertake. Excluded activities include standards setting, product rating, audits, certifications or dispute settlement. Similarly, the IT–ISAC is not a crime fighting organization. The nineteen Founding Member companies of the IT–ISAC, all represented at the announcement, are AT&T, Cisco Systems, Computer Associates, CSC, EDS, Entrust Technologies, Hewlett-Packard Company, IBM, Intel Corporation, KPMG Consulting, Microsoft Corporation, Nortel Networks, Oracle Corp., RSA Security,

Securify Inc., Symantec Corporation, Titan Systems Corp., Veridian and VeriSign, Inc.

The group plans to evolve its information sharing activities over time, starting with IT companies and then moving across sectors. It is also expected that the ISAC will enable sensitive information to be shared between industry and government. But that sharing must be a two-way street, if it is going to be effective.

The Software Engineering Institute's CERT Coordination Center plays an information sharing role for numerous industries. The oldest and largest of information sharing programs, CERT is a Federally funded research and development center at Carnegie Mellon University in Pittsburgh. The organization gathers and disseminates information on incidents, product vulnerabilities, fixes, protections, improvements and system survivability. The organization strives to maintain a leak proof reputation while collecting thousands of incident reports yearly. These could be anything from a single site reporting a compromise attempt to a virus with worldwide impact.

The IT–ISAC is specifically designed to support the IT industry in this country. Other ISACs have been formed in the financial services and telecommunications industries. And I would like to mention two other groups that play an important information sharing role. *The Partnership for Critical Infrastructure Security* provides a venue for organizations from numerous industries to pool their knowledge and experience about information infrastructure risks and protections. PCIS also examines critical interdependencies among infrastructure providers and seeks common solutions to risk mitigation. *The Partnership for Global Information Security* <http://www.pgis.org> provides a forum for executives from both the public and private sector in economies around the world to share information about InfoSec topics. PGIS members are focused on five areas for collaboration: sound practices, workforce, research and development, cyber crime and law enforcement and public policy. ITAA is proud to have played a leadership role in the formation of both organizations, and I sit on the Boards of Directors of both.

Awareness: ITAA and its member companies are raising awareness of the issue within the IT industry and through partnership relationships with other vertical industries, including finance, telecommunications, energy, transportation, and health services. We are developing regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing information security. An awareness raising campaign targeting the IT industry and vertical industries dependent on information such as the financial sector, insurance, electricity, transportation and telecommunications is being overlaid with a targeted community effort directed at CEOs, end users and independent auditors. The goal of the awareness campaign is to educate the audiences on the importance of protecting a company's infrastructure, and instructing on steps they can take to accomplish this. The message is that information security must become a top tier priority for businesses and individuals.

Education: In an effort to take a longer-range approach to the development of appropriate conduct on the Internet, the Department of Justice and the Information Technology Association of America have formed the *Cybercitizen Partnership*. Numerous ITAA member companies and recently the Department of Defense have joined this effort. The Partnership is a public/private sector venture formed to create awareness in children of appropriate on-line conduct. This effort extends beyond the traditional concerns for children's safety on the Internet, a protective strategy, and focuses on developing an understanding of the ethical behavior and responsibilities that accompany use of this new and exciting medium. The Partnership is developing focused messages, curriculum guides and parental information materials aimed at instilling a knowledge and understanding of appropriate behavior on-line. The Partnership hosted a very successful event last fall at Marymount University in Northern Virginia that brought together key stakeholders in this area. Ultimately, a long range, ongoing effort to insure proper behavior is the best defense against the growing number of reported incidents of computer crime. The Cybercitizen website has received over 600,000 hits in the past year.

Training: ITAA long has been an outspoken organization on the impact of the shortage of IT workers—whether in computer security or any of the other IT occupations. Our groundbreaking studies on the IT workforce shortage, including the latest, *"When Can You Start,"* have defined the debate and brought national attention to the need for new solutions to meet the current and projected shortages of IT workers. We believe it is important to assess the need for and train information security specialists, and believe it is equally important to train every worker about how to protect systems.

We have planned a security skills set study to determine what the critical skills are, and will then set out to compare those needs with courses taught at the university level in an effort to determine which programs are strong producers. We encourage the development of "university excellence centers" in this arena, and also advocate funding for scholarships to study information security. We commend the Administration and Congress for supporting training more information security specialists.

The challenge to find InfoSec workers is enormous, because they frequently require additional training and education beyond what is normally achieved by IT workers. Many of the positions involving InfoSec require US citizenship, particularly those within the federal government, so using immigrants or outsourcing the projects to other countries is not an option.

Best Practices: We are committed to promoting best practices for information security, and look to partners in many vertical sectors in order to leverage existing work in this area. In addition, our industry is committed to working with the government—whether at the federal, state or local levels. For example, we are working with the Federal Government's CIO Council on efforts to share industry's best information security practices with CIOs across departments and agencies. At the same time, industry is listening to best practices developed by the government. This exchange of information will help industry and government alike in creating solutions without reinventing the wheel.

While we strongly endorse best practices, we strongly discourage the setting of "standards." Why?

Broadly, the IT industry sees standards as a snapshot of technology at a given moment, creating the risks that technology becomes frozen in place, or that participants coalesce around the "wrong" standards. Fighting cyber crime can be thought of as an escalating arms race, in which each time the "good guys" develop a technology solution to a particular threat, the "bad guys" develop a new means of attack. So to mandate a particular "solution" may be exactly the wrong way to go if a new threat will soon be appearing.

It is also critical that best practices are developed the way much of the Internet and surrounding technologies have progressed—through "de facto" standards being established without burdensome technical rules or regulations. While ITAA acknowledges the desire within the Federal government to achieve interoperability of products and systems through standard-setting efforts, the reality is that the IT industry can address this simply by responding to the marketplace demand. The marketplace has allowed the best technologies to rise to the top, and there is no reason to treat information security practices differently.

Research and Development: While the information technology industry is spending billions on research and development efforts—maintaining our nation's role as the leader in information technology products and services—there are gaps in R&D. Frankly, for industry, more money is frequently spent on "D"—development—then "R"—long-term research. Government, mainly in the Department of Defense, focuses its information security R&D spending on defense and national security issues. We believe that between industry's market-driven R&D and government's defense-oriented R&D projects, gaps may be emerging that no market forces or government mandates will address. Government funding in this gap—bringing together government, academia and industry—is necessary.

International: In our work with members of the information technology industry and other industries, including financial services, banking, energy, transportation, and others, one clear message constantly emerges: information security must be addressed as an international issue. American companies increasingly are global corporations, with partners, suppliers and customers located around the world. This global business environment has only been accented by the emergence of on-line commerce—business-to-business and business-to-consumer alike.

Addressing information security on a global level clearly raises questions. Many within the defense, national security and intelligence communities rightly raise concerns about what international actually means. Yet, we must address these questions with solutions and not simply ignore the international arena. To enable the dialogue that is needed in this area, ITAA and WITSA conducted the first Global Information Security Summit in Fall 2000. This event brought together industry, government and academia representatives from around the world to begin the process of addressing these international questions. A second Summit is planned for later this year to continue the dialogue. The governmental international linkages

must be strengthened—and not just among the law enforcement and intelligence communities. Government ministries around the world involved in economic issues—such as our own Department of Commerce—need to be key players.

How Government Can Help

In many ways, solutions to cyber security challenges are no different than any other Internet-related policy issue. Industry leadership has been the hallmark of the ubiquitous success of our sector. Having said that, we also believe that government has several roles to play in helping achieve better cyber security and combating cyber crime:

- First and foremost, like a good physician practicing under the Hippocratic oath, do no harm. Excessive or overly broad legislation and subsequent regulation crafted in a rapidly changing technology environment is apt to miss the mark and likely to trigger a host of unintended consequences. In many instances, existing laws for crimes in the physical world are adequate to address crimes conducted in cyberspace. New legislation should always be vetted for circumstances that single out the Internet for discriminatory treatment.
- Practice what you preach. The rules of technology, process and people apply equally to the public sector. The U.S. government must lead by example in preventing intrusions into agency websites, databanks and information systems. Leadership in this area means substantial investments of new money in information security technology and services. Responding to the issue by reallocating existing dollars from current programs is robbing Peter to pay Paul and likely to play out at the expense of the American public and their confidence in e-government. It also means insisting that government agencies implement rigorous information security processes and practice them on a daily basis. Making InfoSec part of the government culture will require extensive senior management commitment.
- Reach out to international counterparts for crucial discussions of cyber security, and in particular, how to most constructively and effectively enforce existing criminal laws in the increasingly international law enforcement environment fostered by the Internet and other information networks.
- Bring leadership to bear through existing structures including the new cyber security board that will likely be established by Executive Order later this year. ITAA, its members and the IT industry continue to work hard to develop collegial and constructive relationships with the leadership and staff of the Critical Information Assurance Office (CIAO), the Commerce Department (DOC), the National Institute of Standards and Technology (NIST), and the Critical Information Infrastructure Assurance Program Office (CIIAP) at NTIA, as well as the National Security Council (NSC), Department of Justice (DOJ), Department of Energy, the National Information Protection Center (NIPC), and the National Security Agency (NSA).
- Funding will also help in the areas of workforce development and research. We have a critical shortage of information technology professionals generally and information security specialists specifically. In general, we support legislation to increase the number of appropriately skilled workers in this critical area. We also support additional R&D funding.

Conclusion

Society's reliance on the Internet will only increase over time. The evolution of the Internet over these thirty-some years tells us that its possibilities are limited only by our imaginations. The prospect of ubiquitous commerce, brought about by wireless computing, could pose greater security challenges as we move forward.

Internet security is an enabler to continued progress, and without it, public trust could erode and the true limits of technology never be pushed. I submit to you that the market is moving quickly to establish and maintain public trust in this new and exciting medium.

In closing, I leave the committee with the following thoughts on securing the Internet.

- Internet security must continue to become the focus of corporate CEOs and Boards of Directors and their counterparts in the public sector. Internet security is economic security, and market forces will continue to draw the attention of the highest levels of corporate hierarchy. This is a beneficial development.

- The Internet will continue to evolve towards ubiquity. As it does, technological developments will move quickly to secure it, but implementing those technologies will be essential.
- Technology is only part of the answer. People and processes are the other key ingredients. Assuring that users and companies practice sound "cyber hygiene" is important to securing the Internet.
- Market forces are the key. These forces will prevent an erosion of trust, will contribute to efficiently developing security products, and will drive management at all levels to focus on Internet security.
- Educating young people about the need to be good cybercitizens—through programs such as the ITAA/Department of Justice/Department of Defense Cybercitizen Partnership—is one tool to fight cybercrime that needs wider support.

Thank you and I welcome any questions from the Committee.

Senator WYDEN. Very well said.
Mr. Schneier, welcome.

STATEMENT OF BRUCE SCHNEIER, CHIEF TECHNICAL OFFICER, COUNTERPANE INTERNET SECURITY, INC.

Mr. SCHNEIER. Thank you. Thanks for having us. I spent the entire weekend at DEFCON sort of wondering what I would tell the Committee. It has been interesting, I spent a lot of time talking to different people, and when I got here I actually snitched one of your pads and wrote a bunch of notes.

Kind of the neat thing is, I am listening to your opening remarks, and about five of the points I wanted to make you made to me, so I feel like I am in good company. Now, you said very well, the Internet is important to business, to people. The ramifications of that are interesting, but what we want to do fundamentally is take all of our business and social constructs and move them from the real world to the Net, whether it is having a private conversation, engaging in commerce, having a meeting, political discussions, potentially we are talking about putting everything that we do in the real world on the Net.

Fundamentally, security is the enabling technology, the limits of security are in a very real sense the limits of the Internet. If you cannot do it securely, whether it is you knowing who I am when I speak to you, or me making an anonymous purchase, or voting, we are not going to do it, and this is only going to get bigger.

Now, I have been doing security for, I do not know, 10, 15 years, and what I have learned sort of watching the world and being involved in it is that security is not working. Every year, the problem gets worse. Security is failing us. We see this in all the press reports you mentioned. We see this in how much damage there is, how much money is lost, how many incidents there are. I mean, every metric.

Things are not getting better, despite computer security being a 40-year-old academic discipline, and every year there are new products, new ideas, new services. It is not that we are not winning, we are not even breaking even, and I spent a lot of time writing my most recent book and thinking about the problem, because it is surprising—why are we not getting better?—and I believe fundamentally it is about complexity, and we heard that here, in some ways.

Complexity to me is the enemy of security. As things get more complex, they necessarily get less secure, and our Internet, our electronic world is getting more complex faster than our security knowledge is improving, whether it is always on connections, whether it is rich content, whether it is a new version of Windows, it is more complex, more features, more interactions, more users, and it is less secure.

So what do we do? To a first approximation, the Internet is about people. You said very well that technology alone cannot be the solution, because it is not a technology problem. Fundamentally, it is a people problem. I mean, the same problems we have in the real world we have on the Net. We have fraud, threat, trespass, damage. None of these crimes are new.

Now, also, the Internet is different. There are three main differences that are worth bringing out. The first one is automation. The fact that you can automate an attack, the fact that you can automate a crime, makes certain things a lot easier to do as a criminal, and a lot harder to find.

You know, picking up a penny from everybody becomes a valid way of doing crime on the Net. In the real world, you could never make that efficient.

We talk about the notion of the script kitty, and I think Vint mentioned this, the idea of taking an attack where a skilled person knows how to do it, encapsulating it in software, and giving it to 10,000 people. We have separated skill from ability through automation, and that is a very big difference, and a very big deal.

Another big difference is a lack of political boundaries. All of our law enforcement is based on proximity, an attacker going up to you and hitting you over the head. We know how to prosecute that, but if the attacker starts in Russia and accesses computers in France to get to Citibank in New York, suddenly that is a lot less clear, and things are much more complicated, and this lack of political boundaries makes any security work much more difficult, because you are not dealing with any coherent group.

The third difference is how techniques propagate. Because the Internet is so pervasive in communication, criminal techniques, hacking techniques propagate much quicker, and you can see this in the real world, when a new way of breaking into an ATM machine, for example, is discovered, people learn about it slowly, and the attack becomes in vogue. On the Net, this can happen overnight, so a lot of our traditional ways of dealing with crime, which is fixing it after we see it is a problem, fails when things happen so fast.

So again, to me, I believe Internet security will continue to get worse in the foreseeable future. I do not see any magic bullets. I do not see any ways to solve the problem.

So the question to ask is, what do we do? Given this reality, and I believe 100 percent this is true, what can we do? We cannot shut the Net down. We cannot say, less complexity. I know you think the operating system is fun. We are not going to do that. We are not going to put cell phones in the Net. We are not going to have mobile commerce. They are going to happen, whether they are secure or not, so I have some suggestions.

The first one is something that I am working on in my company, not really something for you to do, is to look at detection response. I mean, I look at security in terms of prevention, detection, and response. A lot of what we have done in computer security is prevention. We have built all of these prophylactics that we assume will prevent fraud, prevent crime, and that is what is failing in the real world. We get security through detection response.

I do not wear body armor, but I am safe on the streets not because I have prevented crime, but because I understand that if there is a crime, that there will be detection response. If you want to improve the security in your house, you do not make your walls thicker, you get a burglar alarm, and to me this is very important. This makes security robust. Right now, security is very fragile on the Net, and you see it in the newspapers. A new vulnerability is discovered, and we are all at risk. Suddenly, we are not secure.

Alarm systems are robust. If you have enough motion sensors and pressure plates and electric eyes in your house, you will catch the burglar, regardless of how he got in, and we need that same kind of thinking on the Net.

The second thing, and you talked about this, and I am thrilled you did, risk management. A lot of us talk about how do we avoid the threat? We cannot avoid the threat. The question is, how do we manage the risk? Just like any other business risk, computer crime and fraud is a risk, and this has some ramifications. I believe the insurance industry will be key in dealing with computer security, just like the insurance industry over the century has been key in safe automobile practices, in building and housing codes, because they are the risk manager of last resort.

In a few years, you will get cyber insurance. You will have to, as a business, and then a few years later, premiums will diverge, depending on what products you are using, what you are doing, and what this will bring is something else we are lacking, is liability.

Right now, there is no liability in software. An automobile manufacturer could, conceivably, put an oxyacetylene shunt into your fuel line and boost the performance of your car. They do not do that because they know the liability to be enormous. The software industry has no such compunctions. There is no liability. If you read software licenses, they basically say, if this product deliberately maims your children, and we knew about it, and we chose not to tell you because we thought it would hurt sales, we are not liable. This is a disaster, because it means that features come unfettered with any controls.

My third piece of advice is about legislation. I worry about rushing into legislation. This is all very new. We do not understand how the technology works, how it interacts, even things like what it means to trespass on a Web site. What does unauthorized access mean? It is not at all obvious.

I am spending time talking with a Stanford law professor trying to write a paper on this. It is very hard to pin down what these things mean in this new environment, and we will figure it out, but it is going to take a while, and I worry about quick laws that have unintended consequences. We have seen that a couple of times.

I also think we really can no longer have laws that trail technology. Up to now a new technology has appeared, the telephone, and over 10 or 20 years we have figured out what the laws are. Technology moves too fast today. We do not have time to do that. This is an enormous challenge because we almost have to make laws that are based on principles, not based on the details of technology, and then that way you can make the technology match what you want.

To a very real extent, technology can determine what laws are possible. There are some things we cannot do on the Net, no matter how much you want, but if we have some guiding principles as to what we as a society believe is good, and right, and important, we can codify that into the actual technology, and to me this is an enormous opportunity for America to take its principles of free speech, personal privacy, of liberty, and weave them into the fabric of a very international Net. We could fail to do that, but we could also do that.

I guess those are my points. I will take questions, and if there is ever a job application for that information security czar, I would love to do it.

[Laughter.]

[The prepared statement of Mr. Schneier follows:]

PREPARED STATEMENT OF BRUCE SCHNEIER, CHIEF TECHNICAL OFFICER, COUNTERPANE INTERNET SECURITY, INC.

My name is Bruce Schneier. I am the founder and Chief Technical Officer of Counterpane Internet Security. Inc. Counterpane was founded to address the immediate need for increased Internet security, and essentially provides burglar alarm services for computer networks. I am the author of seven books on cryptography and computer security, as well as hundreds of articles and papers on those topics. For several years, I have been a security consultant to many major Internet companies.

I'd like to thank the Committee for holding this hearing today. Internet security is an enormously important issue, and one that will become increasingly important as the Internet affects the lives of more people. Simply stated, during the last decade the Internet has transitioned from a technological plaything for a few people to a critical infrastructure as fundamental as the phone system. Internet security has transitioned from an academic curiosity to a fundamental enabling technology for our future. The limits of Internet security are the limits of the Internet, and the limits of the Internet profoundly affect our country as the Information Economy continues to grow.

I believe that there are two questions before the Committee today. The first is whether the Internet is safe enough to conduct business on. The second, if you agree that the Internet is not safe enough, is what we can do to improve the situation. I will focus my remarks on these two issues.

Introduction

The Internet is critical to business. Companies have no choice but to connect their internal networks to the rest of the world—to link with customers, suppliers, partners, and their own employees. But with that connection comes new threats: malicious hackers, criminals, industrial spies. These network predators regularly steal corporate assets and intellectual property, cause service breaks and system failures, sully corporate brands, and frighten customers. Unless companies can successfully navigate around these, they will not be able to unlock the full business potential of the Internet.

Traditional approaches to computer security center around preventive techniques, and they don't work. Despite decades of research, and hundreds of available security products, the Internet has steadily become more dangerous. The increased complexity of the Internet and its applications, the rush to put more services and people on the Internet, and the desire to interconnect everything all contribute to the increased insecurity of the digital world.

Security based solely on preventive products is inherently fragile. Newly discovered attacks, the proliferation of attack tools, and flaws in the products themselves all result in a network becoming vulnerable at random (and increasingly frequent) intervals.

Active security monitoring is a key component missing in most networks. Insurance is another. In business, insurance is the risk manager of last resort. And in most cases, insurance drives security requirements. Companies install a burglar alarm system in their warehouse not because it reduces theft, but because it reduces their insurance rates. As the need for Internet security becomes more universally recognized , insurance companies will begin to drive security requirements and demand product improvements.

The third key component to a secure Internet is law enforcement. The primary reason we live in a safe society is that we prosecute criminals. Today the Internet is a lawless society; hackers can break into computers with relative impunity. We need to turn the Internet into a lawful society, through regular prosecution and conviction of Internet criminals.

The Importance of Security

When I began working in computer security, the only interest was from the military and a few scattered privacy advocates. The Internet has changed all that. The promise of the Internet is to be a mirror of society. Everything we do in the real world, we want to do on the Internet: conduct private conversations, keep personal papers, sign letters and contracts, speak anonymously, rely on the integrity of information, gamble, vote, publish digital documents. All of these things require security. Computer security is a fundamental enabling technology of the Internet; it's what transforms the Internet from an academic curiosity into a serious business tool. The limits of security are the limits of the Internet. And no business or person is without these security needs.

The risks are real. Everyone talks about the direct risks: theft of trade secrets, customer information, money. People also talk about the productivity losses due to computer security problems. What's the loss to a company if its e-mail goes down for two days? Or if ten people have to scramble to clean up after a particularly nasty intrusion? I've seen figures as high as $10 billion quoted for worldwide losses due to the ILOVEYOU virus; most of that is due to these productivity losses.

More important are the indirect risks: loss of customers, damage to brand, loss of goodwill. Last year Egghead.com had a network break-in and it was rumored that a million credit card numbers were stolen. Regardless of how the investigation turned out, some percentage of customers decided to shop elsewhere. When CD Universe suffered a credit card theft in early 2000, it cost them dearly in their war for market share against Amazon.com and CDNow. In the aftermath of the Microsoft attack in October 2000, the company spent much more money and effort containing the public relations problem than fixing the security problem. The public perception that their source code was untainted was much more important than any effects of the actual attack.

And more indirect risks are coming. European countries have strict privacy laws; American companies can be held liable if they do not take steps to protect the privacy of their European customers. While "safe harbor" provisions may provide immediate relief, it will not solve the problem once the European countries realize that their data is not being protected.

The U.S. has similar laws in particular industries—banking and healthcare—and there are bills in Congress to protect privacy more generally. We have not yet seen shareholder lawsuits against companies that failed to adequately secure their networks and suffered the consequences, but they're coming. Can company officers be held personally liable if they fail to provide for network security? The courts will be deciding this question in the next few years.

As risky as the Internet is, companies have no choice but to be there. The lures of new markets, new customers, new revenue sources, and new business models are just so great that companies will flock to the Internet regardless of the risks. There is no alternative. This, more than anything else, is why computer security is so important.

The Failure of Traditional Security

Five years ago, network security was relatively simple. No one had heard of denial-of-service attacks shutting down Web servers, Web page scripting flaws, or the latest vulnerabilities in Microsoft Outlook Express. In recent years came intrusion detection systems, public-key infrastructure, smart cards, VPNs, and biometrics. New networking services, wireless devices, and the latest products regularly turn network security upside down. There are literally hundreds of network security

products you can buy, and they all claim to provide you with security. They regularly fail, but still you hear companies say: "Of course I'm secure. I bought a firewall."

Network security is an arms race, and the attackers have all the advantages. First, network defenders occupy what military strategists call "the position of the interior": the defender has to defend against every possible attack, while the attacker only has to find one weakness. Second, the immense complexity of modern networks makes them impossible to properly secure. And third, skilled attackers can encapsulate their attacks in software, allowing people with no skill to use them. It's no wonder businesses can't keep up with the threat.

What's amazing is that no one else can either. Computer security is a 40-year-old discipline; every year there's new research, new technologies, new products, even new laws. And every year things get worse.

If there's anything computer security professionals have learned about the Internet, it's that security is relative. Nothing is foolproof. What's secure today may be insecure tomorrow. Even companies like Microsoft can get hacked, badly. There are no silver bullets. The way forward is not more products, but better processes. We have to stop looking for the magic preventive technology that will avoid the threats, and embrace processes that will help us manage the risks.

Security and Risk Management

Ask any network administrator what he needs security for, and he can describe the threats: Web site defacements, corruption and loss of data due to network penetrations, denial-of-service attacks, viruses and Trojans. The list seems endless, and the endless slew of news stories prove that the threats are real.

Ask that same network administrator how security technologies help, and he'll discuss avoiding the threats. This is the traditional paradigm of computer security, born out of a computer science mentality: figure out what the threats are, and build technologies to avoid them. The conceit is that technologies can somehow "solve" computer security, and the end result is a security program that becomes an expense and a barrier to business. How many times has the security officer said: "You can't do that; it would be insecure"?

This paradigm is wrong. Security is a people problem, not a technology problem. There is no computer security product—or even a suite of products—that acts as magical security dust, imbuing a network with the property of "secure." It can't be done. And it's not the way business works.

Businesses manage risks. They manage all sorts of risks; network security is just another one. And there are many different ways to manage risks. The ones you choose in a particular situation depend on the details of that situation. And failures happen regularly; many businesses manage their risks improperly, pay for their mistakes, and then soldier on. Businesses are remarkably resilient.

To take a concrete example, consider a physical store and the risk of shoplifting. Most grocery stores accept the risk as a cost of doing business. Clothing stores might put tags on all their garments and sensors at the doorways; they mitigate the risk with a technology. A jewelry store might mitigate the risk through procedures: all merchandise stays locked up, customers are not allowed to handle anything unattended, etc. And that same jewelry store will carry theft insurance, another risk management tool.

More security isn't always better. You could improve the security of a bank by strip-searching everyone who walks through the front door. But if you did this, you would have no business. Studies show that most shoplifting at department stores occurs in dressing rooms. You could improve security by removing the dressing rooms, but the losses in sales would more than make up for the decrease in shoplifting. What all of these businesses are looking for is adequate security at a reasonable cost. This is what we need on the Internet as well—security that allows a company to offer new services, to expand into new markets, and to attract and retain new customers. And the particular computer security solutions they choose depend on who they are and what they are doing.

Detection and Response

Most computer security is sold as a prophylactic: encryption prevents eavesdropping, firewalls prevent unauthorized network access, PKI prevents impersonation. To the world at large, this is a strange marketing strategy. A door lock is never sold with the slogan: "This lock prevents burglaries." No one ever asks to purchase "a device that will prevent murder." But computer security products are sold that way all the time. Companies regularly try to buy "a device that prevents hacking." This is no more possible than an anti-murder device.

When you buy a safe, it comes with a rating. 30TL—30 minutes, tools. 60TRTL—60 minutes, torch and tools. What this means is that a professional safecracker, with safecracking tools and an oxyacetylene torch, can break open the safe in an hour. If an alarm doesn't sound and guards don't come running within that hour, the safe is worthless. The safe buys you time; you have to spend it wisely.

Real-world security includes prevention, detection, and response. If the prevention mechanisms were perfect, you wouldn't need detection and response. But no prevention mechanism is perfect. This is especially true for computer networks. All software products have security bugs, most network devices are misconfigured, and users make all sorts of mistakes. Without detection and response, the prevention mechanisms only have limited value. They're fragile. And detection and response are not only more cost effective, but also more effective, than piling on more prevention.

On the Internet, this translates to monitoring. In October 2000, Microsoft discovered that an attacker had penetrated their corporate network weeks before, and might have viewed or even altered the source code for some of their products. Administrators discovered this breach when they noticed twenty new accounts being created on a server. Then they went back through their network's audit logs and pieced together how the attacker got in and what he did. If someone had been monitoring those audit logs—automatically generated by the firewalls, servers, routers, etc.—in real time, the attacker could have been detected and repelled at the point of entry.

That's real security. It doesn't matter how the attacker gets in, or what he is doing. If there are enough motion sensors, electric eyes, and pressure plates in your house, you'll catch the burglar regardless of how he got in. If you are monitoring your network carefully enough, you'll catch a hacker regardless of what vulnerability he exploited to gain access. And if you can respond quickly and effectively, you can repel the attacker before he does any damage. Good detection and response can make up for imperfect prevention.

And real security is about people. On the day you're attacked, it doesn't matter how your network is configured, what kind of boxes you have, or how many security devices you've installed. What matters is who is defending you.

Prevention systems are never perfect. No bank ever says: "Our safe is so good, we don't need an alarm system." No museum ever says: "Our door and window locks are so good, we don't need night watchmen." Detection and response are how we get security in the real world, and they're the only way we can possibly get security on the Internet. We must invest in network monitoring if we are to properly manage the risks associated with our nation's network infrastructure.

Insurance

Eventually, the insurance industry will subsume the computer security industry. Not that insurance companies will start marketing security products, but rather that the kind of firewall you use—along with the kind of authentication scheme you use, the kind of operating system you use, and the kind of network monitoring scheme you use—will be strongly influenced by the constraints of insurance.

Consider security, and safety, in the real world. Businesses don't install building alarms because it makes them feel safer; they do it because they get a reduction in their insurance rates. Building owners don't install sprinkler systems out of affection for their tenants, but because building codes and insurance policies demand it. Deciding what kind of theft and fire prevention equipment to install are risk management decisions.

The risk taker of last resort is the insurance industry, and businesses achieve security through insurance. They take the risks they are not willing to accept themselves, bundle them up, and pay someone else to make them go away. If a warehouse is insured properly, the owner is significantly less worried about fire or other disasters. Similarly, if a network is insured properly, the owner is significantly less worried about the hacking risks.

This is the future. Concerned about denial-of-service attacks? Get bandwidth interruption insurance. Concerned about data corruption? Get data integrity insurance. (I'm making these policy names up, here.) Concerned about negative publicity due to a widely publicized network attack? Get a rider on your good name insurance that covers that sort of event. The insurance industry isn't offering all of these policies yet, but it is coming.

The effects of this change will be considerable. Every business will have network security insurance, just as every business has insurance against fire, theft, and any other reasonable threat. To do otherwise would be to behave recklessly and be open to lawsuits. Details of network security become check boxes when it comes time to calculate the premium. Do you have a firewall? Which brand? Your rate may be one

price if you have this brand, and a different price if you have another brand. Do you have a service monitoring your network? If you do, your rate goes down this much.

This process changes everything. What will happen when the CFO looks at his premium and realizes that it will go down 50% if he gets rid of all his insecure Windows operating systems and replaces them with a secure version of Linux? The choice of which operating system to use will no longer be 100% technical. Microsoft, and other companies with shoddy security, will start losing sales because companies don't want to pay the insurance premiums. In this vision of the future, how secure a product is becomes a real, measurable, feature that companies are willing to pay for...because it saves them money in the long run. Already some insurance companies are starting to do this.

Other systems will be affected, too. Online merchants and brick-and-mortar merchants will have different insurance premiums, because the risks are different. Businesses can add authentication mechanisms—public-key certificates, biometrics, smart cards—and either save or lose money depending on their effectiveness. Computer security "snake-oil" peddlers who make outlandish claims and sell ridiculous products will find no buyers as long as the insurance industry doesn't recognize their value. In fact, the whole point of buying a security product or hiring a security service will not be based on threat avoidance; it will be based on risk management.

And it will be about time. Sooner or later, the insurance industry will sell everyone anti-hacking policies. It will be unthinkable not to have one. And then we'll start seeing good security rewarded in the marketplace.

Law Enforcement

The primary reason we feel safe walking the streets of our country is because criminals are arrested and prosecuted. In areas where prosecution is less common, the streets are more dangerous. In countries where prosecution is rare or arbitrary, criminals run rampant. This same thinking must be applied to the Internet.

Right now, most criminal hackers can operate with impunity, and they know that. Most Internet crimes are never discovered by the victims. Of those that are known, most are covered up. Of those that are made public, most never result in arrests, let alone convictions. The Internet is still a lawless environment.

This needs to change. Prosecution and conviction of criminals has two effects. One, it sends a clear message to everyone else. And two, it takes the convicted criminals out of circulation during their incarceration. Both of these things act as a deterrence.

One of the best things that happened for Internet security in the year 2000 was the series of high-profile prosecutions and convictions. This has had a visible chilling effect on some hacking groups. But more is required.

This is not easy. The Internet was not designed to aid forensic analysis, and many types of hacks are not currently traceable. Jurisdiction is also a problem; our criminal justice system is not designed to deal with criminals who can be anywhere in the world while attacking someone in another part of the world. But we need to do it.

Conclusion

Network security risks will always be with us. The downside of being in a highly connected network is that we are all connected with the best and worst of society. Security products will not solve the problems of Internet security, any more than they solve the security problems in the real world. The best we can do is to manage the risks: employ technological and procedural mitigation while at the same time allowing businesses to thrive.

Security equals vigilance, a day-to-day process. There are hundreds of technological solutions, but none that will ultimately fix the problem. It's been thousands of years, and the world still isn't a safe place. There is no way to "solve" the burglary problem. There is no device you can buy to prevent murder. No matter how fast technology advances, guards and alarms are still state-of-the-art.

The key to effective security is human intervention. Automatic security is necessarily flawed. Smart attackers bypass the security, and new attacks fool products. People are needed to recognize, and respond to, new attacks and new threats. It's a simple matter of regaining a balance of power: human minds are the attackers, so human minds need to be the defenders as well.

I believe that the Internet will never be totally secure. In fact, I believe that the Internet will continue to get less and less secure as it gets more interesting, more useful, and more valuable. Just like the real world, security is a process. And the processes of detection and response, risk management and insurance, and forensics and prosecution will serve the Internet world just as they serve the real world.

Senator WYDEN. This has been a superb panel. Having specialized in these issues in health for a number of years, I have gone to a pretty hefty number of panels, and this has been as good as it gets, and I really thank you for it.

Mr. Schneier, what was interesting about your last comment, and I am going to have questions for all of you, is that in your past writings, and talks in the past, you had usually raised as the centerpiece of an effort to deal with security this question of alarms and guards. What you have essentially done today is added a new dimension, and that is that there really ought to be consequences for important players in the economy if they are providing insufficient efforts to address security.

That is something I had never thought of, and I will want to explore it with you, because it raises a number of interesting questions, not the least of which is if you are going to have consequences, you have got to have some standards by which you even look at consequences. I think your point about cyber insurance is a very intriguing one, and the question about at what point would people be held liable for insufficient attention to security is certainly an area we will want to explore.

Let me start with the three of you by putting this in the context of Jane and Joe, the typical consumer who is using their computer. They probably listen to this, and they say to themselves, I do not have any secrets on my computer. I am not doing any multimillion dollar commercial transactions. Who would want to steal my recipes and hear about the text of a letter that I sent to Aunt Gertrude? Why should I be concerned about something like this? What would be the response of the panel members, just starting down the line with you, Dr. Cerf.

Dr. CERF. Well, I hope we do not end up with a hear no evil, see no evil, speak no evil situation. This is a very alarming observation you have just made, because it is very common, and it is not just Joe and Jane, it is Frank, who runs the computer center over at the university, who says, we do not have any secret on our machine. Forget the one with the student grades and so on. This is the R&D machine, but there is nothing secret on it, and so I do not really have to protect it very much.

The problem is that that machine becomes a weapon. It becomes a platform. If it can be penetrated and Trojan horse software placed on it, or what some people call zombie software, that software can later be activated by a hacker and used as a weapon against some other target in the network, and so the failure of a person to observe reasonable security practices, in fact, endangers and hurts everyone.

Now, I am not so foolish as to imagine that we will get everyone to cooperate. In fact, security is inconvenient, and I think it is sort of an unfortunate binding there, that if it was not inconvenient, it would not work very well, so we can encourage good practices, we can explain to people why they should have passwords that are not words, but are, you know, some kind of a pronounceable sequence of vowels and consonants with some numbers thrown in somewhere as well.

Or we can introduce technology that creates what are called nonreusable passwords using public key cryptography as a tool, but we

need to have the manufacturers of the software and hardware help us, perhaps by releasing machines configured with more security in them, and you have to deliberately decide to reduce the level of security so that you know that you are doing that.

Sun Microsystems tried that, and to be honest it did not work very well. the customers did not like it, because it required more work, and they all decided they wanted to reduce their level of security in the machine from the buttoned-up form it was in, so the answer is, we need a lot of education for people to cooperate, and maybe we need simpler practices to make security easier.

Mr. MILLER. Let me go back one question. First, on insurance. There already are insurance companies doing what you and Mr. Schneier have discussed. AIG Insurance, for example, is now promoting very actively to its customers that they will actually send out and do a risk assessment to help you fortify your information security practices, and that will affect the risk premium you end up paying, so it has not become as ubiquitous as Mr. Schneier is suggesting. I agree it is a good idea. It is in its formative stages, beginning out there, and of course AIG is one of the, if not the largest insurance company in the world, so it will have an impact.

To go back to your Joe and Jane question, I think the short answer is again an issue that is very near and dear to your heart, which is privacy. When we go out and do surveys, whether ITAA does them or other people, we find two-thirds of Americans, whether you are talking about doing business on the Internet, or whether you are talking about e-government, are concerned about privacy/security, but when you really start to bore down into their answers, into the second-level questions, what they are really worried about is security, whether they give credit card information over the Internet to a vendor, whether they pass that information to a Government agency, is someone going to steal that information, either while it is in transmission, or when it has arrived at its ultimate destination point.

So the reason the individual Joe and Jane should be concerned about it is, we know they are already concerned about their privacy on the Internet. Every survey shows that Some say 70 percent, some say 80 percent. My question is, why aren't 100 percent of people? It seems like they should be concerned about their privacy on the Internet, but the real solution in most cases is security.

If you do not have security, if that information you are transmitting over the Internet or to your friends, or through I-messaging, whatever you may do, can be easily intercepted, or, when it arrives at its destination, if someone can easily hack into that data base, as has been done—for example, even the Davos Forum had sensitive information of some of the world leaders stolen from that data base. That is what really should begin to strike Joe and Jane to understand why this is so important, so they should be just as concerned as a Member of the U.S. Senate or anybody else about this issue.

Dr. CERF. Harris, don't you think we should also remind people that it is not just a matter of technology and security. If a company successfully receives personal information over an encrypted channel that has all been locked up tighter than a drum, the machine itself is well-protected, but the company's policies are to release the

information to anybody that it chooses for business purposes, all of a sudden, all the technology in the world did not satisfy and solve and protect people's privacy, and so there are some decisions that get made, policies that are set that are independent of the actual technology that we also need to be aware of.

Mr. MILLER. Absolutely. Again, Senator Wyden is a leader in this, so I am not telling him anything he does not know, but obviously we believe that full disclosure by all vendors online is absolutely essential. If anybody violates that full disclosure, the FTC or the State Attorneys General should prosecute them, and third we are very excited about the new technology coming online, the P3P, the platform for privacy protection, which will enable basically every consumer sitting at his or her browser to be able to preset a lot of his or her privacy preferences.

Senator WYDEN. We will not start to reiterate last week's privacy hearing. However, part of my concern on the privacy debate, not unlike the security issue, is that unless you can figure out a way to come up with a practical, enforceable set of policies you have got a very difficult situation where the vast majority are trying to subscribe to the rules and the principles, and a handful of scofflaws are inflicting great damage.

We will not go down the privacy route for the purposes of this afternoon. Mr Schneier, your response to Jane and Joe sitting there following this and saying this really did not apply to me.

Mr. SCHNEIER. If you think about it, pretty much every law we have is subject to the bad actor problem, whether it is our murder statutes or anything, so I think we are stuck with that. It is an interesting question, why the average person should care, because in a lot of ways the average person does not. I mean, if you ask them, are you concerned about security, they will say yes. If you ask them, are you willing to be inconvenienced to get security, they will most likely say no, so people do care, but a lot of it is very superficial caring. The reasons stated here are about the right ones.

The fact that your computer could be a launching pad for other attacks, so I have my computer at home, I do not care if someone breaks into it and then attacks some large e-commerce site. This happens again and again. It used to make the papers a year ago, and now it is business as usual.

There is the notion of identity theft. As more and more of our identity goes online, then identity theft becomes easier and easier. As more and more abilities go online, then identity theft becomes more dangerous and more powerful, and it is a large growth area in crime, and breaking into people's computers to steal their identity, their credit card numbers, their birth date, their address, whatever is needed to get credit issued in their name, that is a big worry, and there is privacy. People are concerned about their information getting leaked.

I guess we saw a couple of weeks ago, or last week, Eli Lilly and Company leaked a bunch of names of drug users out in the open, and this kind of thing is a disaster, and this is why the Europeans have very strong privacy laws. We do not. We rely on companies to sort of do whatever they want, and they inform you, and maybe they do, maybe they do not, and maybe you can understand what

they say, but the information is collected and stored, and I worry about this, because once the information is stored, it is vulnerable.

If, indeed, people are concerned about privacy, the information should not be collected in the first place, because now, once it exists—I mean, the two-year-old e-mail appears. The Web site is broken into. So you take precautions, but they do not actually work, so I think my feeling is people are less concerned than they should be because they do not understand what is going on.

The Internet is very, very new. Our intuitions do not really apply. We think that e-mail is like a chat, is like a conversation, until old e-mail shows up, and maybe shows up in a court trial. We do not know what standards to hold different things to.

Senator WYDEN. Since all of you have said Jane and Joe ought to be concerned, why don't each of you state what you would say would be the seven or eight biggest and most important specific security risks for the typical consumer. You have already mentioned e-mail, credit card, and identity theft, but I might have missed some other ones. Dr. Cerf, why don't you start.

Dr. CERF. I am trying to do a bubble sort in my head here. The one that comes to mind, the top, frankly, is password theft, because people do such a bad job of picking their own passwords, and they often will pick one and stick with it forever and ever, and never change it.

Senator WYDEN. My staff always wants me to use Boss, and that always seems to me to be a little obvious.

[Laughter.]

Mr. SCHNEIER. As long as you trust your staff, that is fine.

[Laughter.]

Dr. CERF. I would say, of the various things that allow a hacker to get into an account, that is probably the most obvious, and getting people to choose different passwords for all the various accounts they have to use is very hard. What do they do, they cannot remember them all, so they write them down, and they stick them on a little post-it next to the machine, so we could help them, I think, with better technology.

Something that Bruce Schneier mentioned is, we have not really engaged public cryptography very well. We do not have that system. If we had that technology in place, we could probably allow people to achieve much better security. They would not ever use reusable passwords. They might have to carry a small device that contains some digital information in it. Of course if they ever lost that device, that is their identity now, so we have to protect that, so there is some recursion here, but I would go after that as one place where Joe and Jane——

Senator WYDEN. So let us see, we have got e-mail, credit cards, identity theft, passwords—anything else that you think, Dr. Cerf. Did you not mention something about public access to Government documents? Were you talking about mortgages, and that sort?

Dr. CERF. This is one of those tension things where being able to get to what should be and is legally public information is very attractive, but many people do not expect their house designs, for example, to become visible. They had to be examined for meeting the codes, for example, and so they are on record, but one does not think the same way about those plans and designs and details

until you realize they might be online and available to anyone, including the criminal who is figuring out how to break into your house.

I do not know what to do about that, to be quite honest with you, other than just perhaps say that access to them has to be more restricted than it is today.

Senator WYDEN. And the reason that you do not is, you see the public interest in the disclosure. For example, if you were to look at a United States Senator's financial disclosure form, and various other kinds of forms, we could be very certain that there is a strong public interest in those kinds of materials being online, and what you are saying is that we are not yet in a position to ensure that those are secure.

Dr. CERF. I think that we also have not fully internalized what it means to have so many of these Government records online, readily available and sorted through, and perhaps collated in ways that we could not do before.

Senator WYDEN. OK. Mr. Miller.

Mr. MILLER. I would add something Mr. Schneier mentioned, which is just personal communications. Again, people do not realize that—because it is digital, they do not understand that there is a nondigital form of that communication. They may send someone an e-mail, and they think somehow it vaporizes, the same way as whispering to them in the back of the room.

Well, it is not. Those personal communications in fact do exist some place. In many cases, they exist many places, and those are showing up in surprising places, in courts of law, in the press, when people assume that somehow that thing just disappears, so I think people have to be much more sensitive to those communications.

However, Mr. Chairman, I would say, while I appreciate your focusing on Joe and Jane, I do not think we as an industry want people to think that the individual citizen has a tremendous amount of personal responsibility that requires a lot of time and effort on his or her part in order to be safe and secure on the Internet, any more than when we pick up the telephone, that we think they have to bring out some kind of special encoder before we have a telephone conversation, or before we get in our car every day we have to spend a lot of time putting special devices in.

That is the tradeoff that you were suggesting before. Everyone wants to go as fast as a Ferrari, but we all want to have a Brinks truck safety at the same time, and from the perspective of the individual consumer, we do not want to tell that individual consumer that he or she cannot go very fast on the Internet because we have added all kinds of burdens to the use of the Internet in the name of security, so that is the constant challenge we have, is to make those security features as easy and as ubiquitous as possible, not so complicated people are afraid of using it altogether, or get so frustrated using it that they will not use it at all.

Senator WYDEN. Would there be a world where there could be more Government spending, and we could keep the Government deficit down, and a world where there could be more security and lots of convenience.

Mr. SCHNEIER. With world peace.

Senator WYDEN. Did you want to add anything else?

Mr. SCHNEIER. Yes. Actually, I sort of agree with what Mr. Harris said. There was a security disaster that happened a few months ago, a serious one. My mother got a computer. Actually—this is on the record, right?

Senator WYDEN. She is listening.

[Laughter.]

Mr. SCHNEIER. There are security practices that there is no way in the world she could be expected to do, will do, will understand doing. It is just too different, so we cannot expect the average person to take this matter into their own hands, because that is the average person.

So what other risk—I tried to put them in some kind of order. You talk about passwords. Passwords are not in themselves—some passwords are an entre into getting something else, so I do not like saying that your password is a vulnerability. Your password is the means by which other things are gotten at, and it is stuff we talked at.

It is basically private information, whether it is personal information about yourself, about your life, about things you do, or health information, what your health is, and as we say this, you can imagine who either in industry or friends and colleagues or enemies might want this information, what they might want to do with it. It is not just credit card numbers, it is credentials.

Credit card numbers are a credential by which you buy something, and it is sort of—under that umbrella of credentials is not only credit card numbers, it is your account, in one click. I buy stuff on Amazon with one click. I do not type in my credit card number, and so that password I use to get into Amazon is as valuable as my credit card numbers as far as Amazon is concerned. Different accounts I have, maybe on eBay or other, maybe—there are premium news services I subscribe to. These are all credentials.

Political speech in the United States, that is not a problem. In many countries, political speech is a big deal, and needing to keep that private is a matter of life and death.

One of the major gay and lesbian Web sites regularly has on their Web site people who would be put to death if the fact that they were on the Web site became known, and there are countries where that is illegal, punishable by death.

Going back to commerce, it is purchasing patterns. If you remember, when Judge Bork was not confirmed for the Supreme Court, one of the local D.C. papers pulled his videotape rentals, records from whatever store he went to. The hope was that they were exciting, but very quickly Congress passed a law making those records private.

More generally, your purchasing patterns, whether they are books, whether they are videos, your browsing patterns, what Web sites you look at, how often you spend time there, this is all information that if I told my mother that anybody could find out that, telemarketers could learn and could exploit, she would not be happy, because she expects, just as when she walks into a bookstore and pays for her book with cash, she is anonymous. She wants to be able to go to a Web site, and for that to be anonymous, and that is what is expected.

Senator WYDEN. In a recent news article, gentlemen, entitled, "Microsoft Outlook Vulnerable to New Attack," the author makes a statement that there is an e-mail software flaw that, in his words, could enable an attacker to take full control of a victim's computer. In your view, is that an overstatement? Is that far-fetched? Dr. Cerf.

Dr. CERF. I am not going to be able to respond fully, because I do not have all the details of that particular vulnerability. Mr. Schneier might be able to do that. But on the face of it, it is a pretty serious problem, and it is a classic problem. The word complexity has been used more than once in today's hearings, and by any reasonable stretch, that software and the rest of the software ensemble that makes up the e-mail system of the Internet is large and complex and is subject to holes.

I will say that a responsible company would do two things in providing new software for its customers. One thing, of course, is to add new features and services that the customers want. That is good business practice, but the second thing is to make sure that vulnerabilities have not been opened up either by simple bugs or by abuse. Sometimes you can make very powerful software. Some things you can do amazing things with, but that same tool could become an enormous vulnerability, because someone could exploit it.

I think software companies have to pay attention to both sides of that coin, and I do not believe in general they all do.

Senator WYDEN. Mr. Miller.

Mr. MILLER. I think that is a gross overstatement, if not an outright falsehood. Software companies, including Microsoft and others, focus a great deal on their information security because at the end of the day their customers would not tolerate having to operate on the Internet if they believe there are flaws that are constantly on the system that are not being attended to.

However, I would agree with what both Dr. Cerf and Mr. Schneier said. There is a very complex world, and in a sense the information security challenge is, it is an arms race. Every time a company comes up with a solution to a particular flaw, or problem that is identified, then the bad guys go out there and try to find other flaws, or other problems. It is not a fixed situation, as it is in the physical world, where once you have put your fence in and bought your dogs and electrified your operation, you are pretty much comfortable with where you are.

So it is a constant challenge. That is why companies like Microsoft and others devote so many of the dollars resources to fighting this challenge, and why they are going to have to be, as Mr. Schneier said, eternally vigilant, otherwise we are going to constantly have these problems.

Senator WYDEN. I think that is a good point. I know there is a hack attack Web site, and a variety of places where people look constantly to do just exactly what you are talking about, which is to move several steps ahead. I very much appreciate that comment.

Mr. Schneier.

Mr. SCHNEIER. I am a little less optimistic. Taking Microsoft as an example, every time there is a new version of Windows, they

will tout how much they spent on security, how much time, how much effort.

For Windows NT, the number was 500 man-years of testing, which includes security, and this was the most secure operating system ever, and every time the press asks me what I think of that, and every time I say, this will be the least secure operating system Microsoft has produced, and every time that happens to be true. As it gets more complex, as it gets bigger it gets less secure, and now they are touting the new version of Windows, and all the security in there, and I believe we will come back here in three years, and we will see it as the least-secure operating system they have ever produced.

You mentioned the news report, and I actually do not know which one you are talking about. If you actually follow this, there are 50 to 60 new vulnerabilities discovered per week. Some of them are minor and obscure, some of them are as bad as the news headline you read indicates.

There are regularly vulnerabilities in that Microsoft product that are that severe. There are regularly vulnerabilities in other products that are that severe. This is software This is the way software works. This is the way software is developed. It is actually a very tough problem. As a business, the way software is secured is the notion of, you throw it out there, hackers find these vulnerabilities, they issue them to the press, or maybe tell the vendor, and then the vendor patches them.

Now, it is an interesting notion—and it used to sort of work, it does not any more, and again it is because of complexity. There might be a dozen or so patches that come out every week in major software products, and maybe half a dozen apply to you. This means every day you are expected to install a patch in your network, and you are actually expected—many news reports read on the order of, his patches were not up to date, he deserved to get hacked, which to me is very much blaming the victim. You know, she walked down that darkened street. She deserved to get mugged.

I do not buy it any more. The Net is getting so complex that this notion of patching is failing. We are losing ground, and we see lots of hacks that happen based on vulnerabilities that have been patched. There are a plethora of worms around Christmastime that attack versions of Linux that should have been patched. The FBI announced, I think in March, the East European thieves who were breaking into Web sites stealing credit card numbers, and extorting companies. Those are vulnerabilities that should have been patched a year earlier.

One of the first big credit card thefts was CD Universe. This was back when these things made the newspapers. That was a vulnerability that was patched a year and a half ago. It was a Microsoft vulnerability, and the company did not install the patch.

A number of the Government break-ins are a patch that should have been installed, so there are vulnerabilities that are that serious, and they are out there, even if they are patched. Companies are still vulnerable three years later.

Senator WYDEN. That is a good response. I was struck again, in reviewing some of the latest literature, that there does seem to be

some evidence that people actually target patches, because they see that as a weak point. I appreciate your comment.

Mr. Miller wants to respond.

Mr. MILLER. One thing Mr. Schneier said earlier I do disagree with slightly, although I do not think it undermines the fundamental point all three of us are making, is that he said something to the effect of by no metrics are we getting more successful than we were, because if you look at all of these numbers in absolute terms, the amount of dollars stolen reported by the Computer Security Institute, the number of attacks that take place, et cetera, they have all been going up, they are trending up, and that is certainly accurate, but what Mr. Schneier's comment does not take into account is the denominator.

We are talking about a tremendously widened use of the Internet, and so I do not know that it is true—in fact, it strikes me probably is not true, that as a percentage of all financial transactions on the Internet today, we are doing a worse job than we were three years ago of preventing credit card information from being stolen, for example, so it is a little hard, I think, to say that under no metrics are we doing better.

I am actually inclined to think that as a percentage, because the Internet itself and all of these governmental uses is expanding so dramatically, that we can get carried away by saying, well, last year it was $300 million that was stolen according to the Computer Security Institute, this year it is $400 million.

First I guess that number is way low. That is the only people reporting incidents. That probably does not take into account the huge number of people who never report the incidents that occur anyhow, but even given that, I think in terms of as a percentage of overall transactions we probably are actually doing better, not worse.

Again, it does not undermine the fundamental point that information security needs to be a higher priority.

Senator WYDEN. We are about to trigger a very vigorous debate now.

Mr. SCHNEIER. Actually, he is basically right.

Senator WYDEN. Dr. Cerf wanted to comment also. I wanted to recognize, in fact, before we have your response, that Senator Nelson has joined us. He and I go back some 20 years, since our days in the House, when I had a full head of hair and rugged good looks.

We are so pleased that Senator Nelson has joined us on this Committee. He has a long interest in technology and science questions. Bill, would you like to make any comments?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. I should have been here two hours ago if the airlines had done their job.

Senator WYDEN. We can talk about the airline passenger bill of rights another day.

Senator NELSON. As a result of my experience today.

Senator WYDEN. We are glad you are here.

Dr. Cerf, on this point that we are exploring with respect to Mr. Miller's last comment——

Dr. CERF. Actually, I had two comments, maybe three now. As of this morning, I had a full head of hair, but in the process of fighting all the problems of computer security I no longer do.

[Laughter.]

Dr. CERF. Mr. Harris' comments draw to mind the phrase, your mileage may vary, and the degree of security that we achieve will probably vary from one company to another and one installation to another. I am a kind of techno-optimist, to try to counterbalance Mr. Schneier. However, his point is extremely well-taken.

No matter how careful you are to fix problems in software, and there always will be problems, getting people to implement them is hard, and so one begins to wonder—and this is the optimistic side of me. One wonders if we cannot do more to automate the process of keeping the software up to date and repaired.

It is not a trivial exercise, and we had at least one embarrassing incident where a person other than Microsoft registered the ability to digitally sign some code that looked like it came from Microsoft. I do not think anything bad actually came of it, but the potential was pretty severe.

So looking for ways to safely automate the process of keeping software up to date would be a very attractive goal if we could figure out how to do it.

Senator WYDEN. That certainly is sensible from my vantage point, because what it is about is ensuring that, at every step, we are minimizing risk. What we are trying to do is say, these are the tools that we have available to us at this time, recognizing that it is not a risk-free world. It is not a risk-free world online, and it is not a risk-free world offline. In that sense, there is some common ground with the three of you.

Let me turn now to the business side specifically, because I tried to talk initially about the typical consumer. When determining whether or not to conduct a transaction online, gentlemen, how can an e-consumer judge whether a business is managing risk properly? As of today, Dr. Cerf, how does a consumer make that assessment?

Dr. CERF. I do not think there are any more or better metrics for users today than there were pre-e-commerce. One wonders—for example, I buy merchandise from some store, how do I know that the store has tried to make sure the merchandise is of good quality or not? Well, I do not have a good way to know that, but I consult Consumers Review, and I consult my friends, and I consult the business pages, I consult the Better Business Bureau.

I suspect that tools of that ilk will be common for the e-world, just as much as they have been helpful in the real world, but I do not have a finger to point.

There is one interesting thing, however. Look at eBay, an interesting lesson that we can learn from that. The providers of goods, and the purchasers of those goods, are just ordinary folks like you and me and they encompass the full range of our human race, including people who are cheating and people who are quite sincere. eBay has built in a feedback mechanism that lets people know what others' experiences have been.

I am not sure that that can apply in all cases, but the notion of consumer feedback, visible to other consumers, is pretty fascinating

to me. I think there is one company called Bizrate that is invited by some companies to interrogate users after they have completed the transaction, or a consumer, to find out whether the consumer was satisfied, and if not, why not, and that information is reported back to the company. It might be reported by Bizrate back to other consumers.

Senator WYDEN. In effect, it puts the company on its toes.

Dr. CERF. Exactly.

Senator WYDEN. Mr. Miller.

Mr. MILLER. We are very fortunate in the United States in these early days of the Internet that financial intermediaries are actually assuming a tremendous amount of the financial risk, and by the way, this is not true outside much of the United States, but if you, as a consumer, go online and order something online using your credit card, and for some reason the process falls apart, you do not get what you wanted, or you cannot settle, usually the credit card company will have your maximum liability at $50, or in some cases liability at zero, so in a sense the risk has been transferred there by the credit card companies to themselves in order to encourage you to go online, and even eBay and some of these other online auction services are now going in that direction.

They in a sense escrow the money for you at certain levels. I believe it is $250, so should that product you were expecting not be what was advertised, instead of a Mickey Mantle baseball, that it is just a baseball, that they bought at Rawlings that day, that your check which you sent for $5,000 does not get forwarded on to the person who sold you this under fraudulent circumstances, and so we are very fortunate to have that kind of protection for people in the online world.

Nevertheless, even with those protections, there still is fraud on the Internet, as Dr. Cerf said. There still are problems on the Internet, and I think what we need to focus on here, Mr. Chairman, is much more vigorous enforcement by our law enforcement agencies, the Federal Trade Commission, State Attorneys General, and I have already seen some references by the new Chairman of the FTC, who I am supposed to be meeting with later this afternoon, that that is one of his priorities.

Third, I very much think the other point Dr. Cerf made about these ratings systems are very, very important. If you go on to some of the very popular Web sites like Yahoo, and they will refer you to a list of merchants from whom you can buy certain electronic products, or CDs, whatever it is online, they have a very sophisticated rating system that they monitor very carefully, because they feel they are tied to that rating system.

Now, you as a consumer may choose to ignore that rating system that you do not care, you just want the lowest price, and even though Yahoo has not given that any rating based on feedback of its customers, you may choose to buy anyhow, but at least there is an attempt on the Internet to constantly create that loop, and one of the beauties of the Internet is that you as a consumer can instantly change, if you are unhappy with Barnes&Noble.com you can switch to Amazon.com in a second. You do not have to worry about whether one is 5 miles away, as opposed to one being 50 miles away. Distance is now gone on the Internet, and one is just

as close as another, and so that is another incentive that acts as a check on consumer problems.

But again, I do not think we should pretend there is no consumer fraud. What we need to make sure is, the Government has the appropriate authority and the appropriate resources to go after those cases of fraud.

Senator WYDEN. Mr. Schneier.

Mr. SCHNEIER. What I first wrote down when you asked the question is, he is screwed. Technically, that is true. There is no technical way the consumer can figure out whether this particular vendor is reputable, will protect their privacy, will sell them good products, will uphold their end of the contract. The mechanisms people use are the same as they use in the real world. If you listen to what Mr. Miller said, it was actually very interesting. The credit card company is taking the liability, and that liability transfer acts as a substitute for good security.

If the credit card company takes liability, I do not care if the vendor behaves rationally. I could buy something online, they do not deliver it, I call my credit card company up, and they reverse the charge. I mean, I have inconvenience, but there is an example of a risk management way of solving a security problem that did not involve any technology, and we do that in the real world all the time, and we are going to do that online.

Dr. Cerf talked about—the name of the thing he talked about is reputation. We use reputation a lot when we make buying decisions. We make all sorts of social decisions. When I walk into a restaurant I actually do not check the health certificate. I assume that it is going to be a good restaurant. Maybe I hear from friends. The reputation of the restaurant will precede it, and occasionally I get it wrong. I have gotten sick from meals. But the social reputation is extremely important.

This is slightly different on the Net, because the Net is global, and there are more companies out there. Only the biggest brands have their reputation. There are millions of little brands, but some of them are aggregating into larger—I mean, you mentioned the Yahoo brands. Amazon has a similar program, where individual companies go under their rubric and can be an Amazon trusted seller. I forget the name it has.

So these are the sorts of methodologies. One of the differences is, in the real world, when I walk into a store, let us say I walk into a McDonald's, I know it is a McDonald's. I see the signs. It looks like a McDonald's. On the Net, it is much easier to forge trade dress.

You can set up a Web site, I can set up a Web site that looks exactly like eBay. It is a perfect replication, and you could come to it, and you would not know. I would be stealing, basically, all of eBay's reputation in an effort to defraud. This has happened. It is not common. I suspect it will get more common, because you do not have the physicality you have in the real world.

So last, I would definitely want to echo what Mr. Miller said on enforcement. To me, this is important. I talk about prevention, detection, and response. The feedback of the mechanism for all of that is deterrence.

One of the best things to me about the year 2000 are in this country the very high-profile arrests and convictions. The Net is still very much a lawless society that you can hack with impunity. The odds of you getting caught are infinitesimal, and to change it, we need to bring the rule of law to the Net, and the way you do that is, after detection and response, after the alarm goes off, forensics, prosecution, conviction, and all of that will give us a safer Net.

We have had problems over the years. we have had overreaction. We have had punishments that do not fit crimes, but to me enforcement is extremely important in giving us a safe world. That is why I am safe when I walk around the streets, not because I am wearing body armor, and not because I have a bodyguard, and not even because I have an alarm, but because I know that the police are out there, and the police have taken crime off the streets.

Dr. CERF. There are a couple of observations. One is, the antidote for bad information in the network environment is more information, and when you discover a hoax or a fraud, there are Web sites out there that make—I do not know that they make a business, but they make a practice of supplying information about those hoaxes and frauds, and sophisticated users who know about that can go to them and check. I imagine any number of people in this room have received the infamous variations on Notes from Nigeria, describing the $25.6 million which is left in some bank account which is being transferred out of the country.

Mr. SCHNEIER. You know that fraud is a few hundred years old. It is called Spanish prisoner. There is nothing new on the Net.

Dr. CERF. In any case, the knowledge that that is a hoax is a helpful thing.

The other thing I wanted to raise a little caution about, the enforcement idea. It is possible to go overboard and try to do the impossible. At one point, a person whose name I will not mention in a fairly public setting wanted me to find a way to ring a bell on the routers every time a packet carrying copyrighted material passed through the router.

I had two reactions to that. One is, the bell might be ringing incessantly and you would not know what to do about it, but—so much for Mr. Schneier's alarm, but the second point is that you might not even know if something was copyright, because when you are looking at the packet level you might see just the words, "call me Ish," and the next packet would say, "mael," and if you could put them—you might know that is the beginning of Moby Dick, but even if you figured that out down at the packet level, you would not know whether the party that was sending the object had the right to do it or not, and certainly when you are moving trillions of packets through the network you do not have time to stop, wait just a moment, I have to do a validity check to find out who owns the copyright on Moby Dick.

So we have to be very cautious now about the notion of enforcement in the presence of such rapidly growing huge scale, and so our mechanisms cannot be to capture all of the information there is to know about everything in the network and record it as an audit trail in case something bad happens. I think we need to do more or less what I believe Mr. Schneier was suggesting, is find a

way to alarm conditions that are visibly bad, or in fact we have to wait until somebody says, there is fraud out there, or I was treated improperly, and that is the alarm, and then we try to go into action.

Senator WYDEN. Let me recognize Senator Nelson.

Senator NELSON. Mr. Chairman, in his statement Dr. Cerf has said that tools for combatting criminal use of online systems may erode privacy in severe ways during the process of trying to assist law enforcement. Have you already discussed his examples of some of those tools?

Senator WYDEN. Not directly, Senator Nelson. I think it is a very good question. We have sort of tangentially talked about the relationship of privacy and security, but Dr. Cerf, I think Senator Nelson's point is a very good one. Do you want to add to that?

Dr. CERF. Indeed it is, Senator Nelson. It is something that all of us worry about. In our zeal to capture the criminal, we may put everyone in jail in some sense by attempting to lock up our society. I do not think anyone in this country wants that.

We need, though, to have tools available. It is just that they have to be applied in a way that was mentioned earlier under the rule of law, under appropriate circumstances, with the appropriate constraints, and perhaps even more important for our system of justice, the data collected has to be collected in a way that maintains the chain of evidence, and that is a delicate and not so easy matter to preserve, so there is, I think, a great deal of care that has to be taken in the exercise of those tools, but we need them.

Senator NELSON. Can you give us an example of some of those counterproductive tools?

Dr. CERF. One of the most visible and perhaps even notorious ones came out of the FBI. It was once called Carnivore. It is called DCS–1000, and I happen to believe that, properly used, that is a very powerful and suitable tool. In fact, it is under better control technically than the classical piece of equipment that we all use in the networking world called a protocol analyzer, which is something that simply swallows every bit that flies across the circuit and analyzes it to tell you hat protocols are in use and what packet contents there are.

Those tools are regularly in use for debugging problems, and you need them for that, but wholesale application of such a tool without the kinds of constraints that I understand have been applied to the FBI system would be a terrible invasion of privacy.

Senator NELSON. So would you, then, suggest that aside from law enforcement agencies in the commercial world, that we not employ those tools?

Dr. CERF. No, I would not say we should not employ them. I would say that they should be employed, but only under proper circumstances, under the authority of a court, for example, in the same way that we would do for the older system of wire taps in the telephone system.

Senator NELSON. In your opinion, do the criminal laws need revision to give law enforcement updated tools to go after this new type of high tech criminal?

Dr. CERF. I have to plead incompetence, Senator. I do not know the answer to that, and I do not think it would be wise for me to

answer it and give you bad data. You would get an opinion, but it would not be a very well-informed one. Perhaps one of my colleagues would be better prepared.

Mr. MILLER. Senator, there is actually a matter that addresses directly Dr. Cerf's point that may come before the Senate very soon, and that is the Council of Europe Cyber Crime Convention, which you may have heard about. About two years ago, the Council of Europe, of which the U.S. has an observer role, decided to achieve a good purpose, we believe, which is to try to develop a convention that would be adopted throughout the world for basic criminal laws to enable there to be existing laws against various cyber crimes.

As we know, in the Philippines, at the time that the ILOVEYOU virus as initiated, the Philippines did not have on its books at that time laws that would enable the Philippines Government to prosecute the individuals when they tracked them down, and they were able to track them down, but they could not do anything with them. The Philippines, to its credit, has updated its laws.

The problem with the cyber crime convention, which has now been virtually finalized, it was developed primarily by law enforcement, with very little input, very untransparent system, very little input by the privacy community, very little input by the consumer community, very little input by the business community and, as a result, while that treaty has some excellent provisions in it, and we still think it is a very good idea, there are many privacy groups, virtually all the privacy groups I am aware of, and some business groups, and some consumer groups, which are uncomfortable with that convention.

Again, it is not to say it is a bad document, but had the Council of Europe worked a little more assiduously to be a little more inclusive of the stakeholders, they probably could have gotten virtually, if not unanimous support for the convention, which would have then been brought to you as Members of the Senate, and your role as ratifiers of treaties, and to other bodies, legislatures around the world, a document that could have become a standard.

Because I think the answer to your last question is, well, we do not believe the U.S. laws by and large need to be changed. There are a lot of other countries around the world where there are huge holes in the abilities of those countries to prosecute cyber criminals, and most of the work to be done is not necessarily in the U.S. Code, or in State laws. Most of the work to be done is around the world.

Dr. CERF. Two very quick points. One of them is that the cyber crime legislation appears to run afoul of cyber privacy legislation in Europe, and I do not know that they have resolved that yet.

The second observation goes with something Harris was just saying. Everything that you do, every law you pass associated with cyber-related matters plainly has jurisdiction in the continental United States and Hawaii and other protectorates, but it does not have jurisdiction in other countries. For this to work on a global scale, there will have to be some degree of collaboration and work to make the laws at the national boundary somehow be at least compatible so that law enforcement can work across international boundaries.

This is not new. It is just, perhaps, made more visible, more highlighted by the global nature of the Internet.

Mr. SCHNEIER. Can I address that question?

Senator WYDEN. Absolutely.

Mr. SCHNEIER. Fundamentally, the tools we are talking about, the tools are to try to balance security versus liberty, and a lot of these tools that come in question are tools that basically take the approach of very broad surveillance in the event at some future time that becomes relevant, so on the Net it might be sucking down every packet looking for copyright violations, or photographing every person going into the Super Bowl in case they had committed a crime.

In the real world there are controls. I mean, I do not believe police are allowed to stop every car and run the license plates. There needs to be some probable cause, so these tools that are potentially dangerous are the ones that do not make the minimization efforts that violate everybody's liberty in an effort to catch a few criminals.

Now, there are countries that do this. This is the rule of law in many countries, and we get to decide what our balance is. What is due process? When is search allowed? When is seizure allowed? This august city has spent 200 years figuring out how this works, and my hope is you guys continue to do so, because they are not easy questions, but that is where all of these tools go in.

To your question about laws, I actually do not believe we need new laws. We need old laws applied cleanly to the new environment, because the crimes are the same, the people are the same, the environment is the same. The techniques are different, but you do not want the same crime to be suddenly much worse or much better if a computer is used. Fraud is fraud, theft is theft, and just because the tool is different does not mean the ramifications should change, and I made this one before you arrived.

We are coming to an age where technology is changing so fast that we cannot make laws that only apply to a certain technology. We are going to forever be playing catch-up. The criminals will work faster than Washington, so we need laws that will stay ahead.

Senator NELSON. Generally, I would agree with you, but in the late seventies that was not the case. When the computer was just coming to be ubiquitous, the prosecutors really did not have the tools at that time. I say this simply from my own experience of having the first computer crimes law in the country in 1978, in the State of Florida, and then having to come up here after the election of 1978. It took me a few years, but we finally got the computer crimes law into the Federal code.

But, I would probably agree with you on your assessment now that there is enough basic criminal law that you can apply to these new high tech crimes.

Mr. Chairman, thank you very much for having a very stimulating discussion.

Senator WYDEN. Senator Nelson, thank you, and again we are so pleased you are going to be on this Subcommittee.

Gentlemen, just a few other questions. One that I want to examine is the impact of technological developments on security issues.

Let us start here with the area of always-on broadband connectivity. I am interested in your thoughts about whether this is going to cause additional security problems. Again, I think part of this whole debate also gets you into Internet-enabled phones and other wireless Internet devices.

Let us start with some of the technological developments such as always-on connectivity, and the new phones. Dr. Cerf.

Dr. CERF. Well, one of the things we have already seen is the invention of something that was not part of the original Internet architecture, a thing called a "firewall." It is intended to shield things that are on the inside from the rest of the unwashed public Internet, and for many years, at least in Internet terms, firewalls were typically applied to the host computers of the network, the ones that supplied the services, but now we are starting to find that individuals with their personal computers that are on all the time connected by digital subscriber loops, or cable modems or the like, need to have firewalls to protect that computer, or maybe an ensemble of computers that happen to be in use at home, or in a small office, from the same kinds of attacks that the host computers were subject to in the past.

But what has happened is that as the functionality available to the consumer increases, then the risk that it will be damaged or interfered with or modified goes up. There is more risk associated with the more functional capability that we now have in these small laptops and personal digital assistants.

I do not know that we need to have firewalls built into our cell phones exactly, but many of us who look at these small devices believe that they need to be created and programmed with the idea in mind that they, too, might be the target of abuse as opposed to simply being a consumer device that is at the edge and no one would ever look at it, so firewalls, and integration of firewall technology into these devices I think is going to be much more common.

Senator WYDEN. Mr. Miller.

Mr. MILLER. What he said.

Senator WYDEN. Mr. Schneier.

Mr. SCHNEIER. My rule of thumb is, if it is a new thing, it increases in security. Always-on connections are less secure than dial-up connections, so when we are talking about always on, or Napster, and other pier to pier, when you are talking about Internet telephony, all of this functionality increases the complexity and will increase in security, and that is just the nature of the beast, and the question is, how do we deal with this?

In some ways we cannot. A lot of these solutions, and these are denial of service attacks, problems, these are the viruses and worms problems, a lot of these solutions are sort of, the draining the swamp variety. We are going to fix the problem by fixing all of these—how many hosts were there? You gave a number, so many millions of hosts.

The problem is, the swampland is being created so fast that we cannot keep up with it. My mother got a computer, and now all of her friends have one. I will put up a personal firewall. I cannot get her to.

So yes, things like always-on connections do increase the risk, and they increase the risks in areas you do not realize. If you re-

member last February, February of 2000, the big denial of service hacks, the first ones that made the newspaper against CNN and eBay and Amazon and a bunch of other Web sites, what we learned very graphically is that if you are the security manager at eBay, your security depends on the security of the University of California at Santa Barbara.

Because it is one big Net, your security depends on other people you cannot control. Right now, the security of your computers, the Senate computers, depends on all of those always-on connections. It depends on people like my mother, and that is pretty scary.

Dr. CERF. In fact, Bruce, I hope we can make it not the case that we have to rely on everyone, those billions, some day, of people on the Net, and we have to do that in several different ways. We have to make it easier for people to have protection. That means building it in as not an afterthought or an add-on, but as part of the design.

An example that you brought up, Bruce, was what is called peer-to-peer exchanges. Napster is an example of that, and Instant Messaging is another example. People like to share things with each other, and the act of sharing means you have to be open to exchange information. You have to allow another party sort of into your inner sanctum.

It would be nice if we had good tools for authenticating those other parties before we opened the door and allowed the peer-to-peer exchanges to happen. We have got pretty good assurance that the party at the other end is the one that we want, and this lets me bring up something that has caused me great difficulty in legislation.

There was a spate of digital signature acts passed both at the State and at the Federal level, and on the one side it is wonderful, because it means people are waking up to the need for this kind of legislation to make digital signatures a real thing in the eyes of the law.

The dismay comes from what appears to be an absence of any standards as to how that digital signature was bound to any individual. What identification did I ask for before I generated the digital signature certificate and associated it with that person, and so far as I can tell, either you have no common standards at all, and sometimes there is nothing even said about validation, and so someone could show up and hand me a thing that is digitally signed, and I have not the foggiest idea whether I can rely on it to mean anything.

So as a kind of small flag-waving exercise, it is very important, if we are going to pass legislation like that, to try to take care of all aspects of it, including the part that says, and by the way, here is how we will rate the quality of the validation.

Senator WYDEN. As the Democratic sponsor of the digital signatures law, I both agree in part and disagree as well. Certainly, we left some of the details to be filled in. We did it largely because technology companies, consumers, and others said, let us make sure that there is a wide enough berth so as to not freeze innovation. I think this is going to be one of the biggest challenges, as we look at these legislative issues down the road.

We are trying to be very sensitive to your point about doing no harm. I think you will hear that from one legislator after another, Democratic and Republican when you make that a particular focus. In this case, the consumers wanted the ease of a digital John Hancock, and the insurance companies and financial services company wanted to simplify their records.

There was a lot of interest in this issue. There was also a feeling that, (a) even if you left some of the details that you are discussing blank, you would not do any harm, and (b) you would have a chance to flesh it out. What you have told us is that you may end up doing some harm as well with people not being sensitive to all of the ramifications. Suffice it to say, by the time you get back home my staff will be on the phone to you about the digital signatures law.

Mr. Schneier.

Mr. SCHNEIER. A couple of points. The idea about authentication brings up some of the main issues. If we decide that authentication is important, we give up anonymity, which is a right that our country believes in, so every time we make decisions we have to balance them with what it is we are trying to do.

This is back to my point that we should try to be technologically variant. We should try to figure out what it is we want, and then apply it to the technology.

You asked about the security of computer telephony. I did not bring it with me, but actually I finished an essay on computer telephony and security. I would be happy to send it to you and, since it came up, I also have any number of essays on digital signatures and authentifications, and the good, bad, and the ugly, so I am willing to inundate you or the record, if it is possible, with paper.

Senator WYDEN. We would very much like both your general essays and the ones on digital signatures.

Senator WYDEN. Mr. Miller, just one point, because you touched on this issue earlier—I gather your companies are going to put much more emphasis on security issues in the future. I saw one study in preparing for the hearing that indicated that even though we are going to see $65 billion this year in online purchases, only 4/10ths of 1 percent of a company's revenue is now dedicated to information security. To your credit, you have indicated several times today that this is going to be an area that your members and businesses generally try to turn around. I think it is clear that is important.

Mr. MILLER. Well, again, Mr. Chairman, that is a very important point, but it is not just the Internet companies, it is the users of the Internet, and that is where we see a tremendous variation. We see industries like the financial services industry, which of course is extremely sensitive to security and reliability, and is heavily regulated by Government regulators, which devotes upwards of 10 percent of its IT budget each year to security, so whenever they are spending $1,000 on computers, whether it is hardware, software, whatever it is, $100 of that is going to be related to security, but there are plenty of other industries that are spending less than 1 percent, and so they are just not focusing so much on it. They have not bought into it.

A lot of it has to do with best practices in industry, a lot of it has to do with the insurance industry, which Mr. Schneier and I have raised, but a lot of it just has to do with volume, Mr. Chairman.

As you know, it was in the lead of Y2K, and back in 1995, we worked with you very closely, we held many Y2K hearings, and meetings in very small phone booths. We just could not get the executive level buy-in that we needed. We could not get the CEO's. We could not get Governors. We could not get mayors, we could not get the top level of Government, and through people like you speaking out, political leaders and business leaders, we eventually did get that kind of level of buy-in.

We need to get the same thing here. Again, it is not enough. It is the CEO's of IT companies. It has to be the CEO's of retail stores, the CEO's of manufacturing firms, the CEO's of pharmaceutical firms, the CEO's of energy firms saying information security is important, and I think that that again is going to be reflected even upward to the President of the United States.

And I think President Bush, like his predecessor, has put a lot of attention on this. We are seeing a new stage in development under President Bush, where he is trying to pull this together in a much more coordinated fashion, and I am hoping that will send the right signal to the CEO's and to the political leaders around the country.

Senator WYDEN. Before we wrap up, gentlemen, I want to recognize in the audience—I think they are still here—the two representatives of the Tunisian Digital Certification Agency. Where are they?

[A show of hands.]

Senator WYDEN. We are glad you are here, and look forward very much to working with your Government on these issues that are worldwide in nature.

Gentlemen, this has been an excellent panel. It is exactly what I hoped to have in terms of our first hearing of this Subcommittee, and suffice it to say, we have a lot to do.

I deliberately steered clear of some of the articles and the quotes of a pretty alarming nature that have been written on this subject. There are various people who are talking about Internet Chernobyls, claiming that we are living right on the edge and the like. I think a point that Mr. Schneier has made both today and in his writing is that people talk very often about those problems offline, as well. We are not seeing mass murderers every single day, fortunately, offline, because there are precautions being taken in that regard. All three of you have made it clear today that you want to be part of doing that online as well.

This is heavy lifting. It is, as you all have said, a tremendous challenge, because we all love the vibrant, open, convenient nature of the Internet. The ability to get all of this information so quickly, and to do what would literally have taken weeks in the past, is an exhilarating, exciting aspect of our lives today. At the same time, we all want the maximum amount of security.

I have found this to be very helpful. You have given us excellent testimony. We are going to keep the hearing record open for two weeks. I think some of my colleagues may want to ask you ques-

tions in writing. Please know that as someone who has really tried to focus on these issues here in the U.S. Senate, I think it has been very, very helpful to be able to have this at a time when clearly the public and private sector need to be more involved, and Mr. Miller has indicated that that is going to be the case. With your leadership, Dr. Cerf and Mr. Schneier, in terms of keeping us up on the state-of-the-art, so to speak, I think that Congress is going to be anxious to work with the private sector to address these issues. Unless you all have anything further, we will adjourn at this time.

Gentlemen, anything further?

Dr. CERF. Nothing from me, Mr. Chairman.

Senator WYDEN. The Subcommittee is adjourned.

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

APPENDIX

PREPARED STATEMENT OF DAVE MCCURDY, PRESIDENT,
ELECTRONIC INDUSTRIES ALLIANCE

Chairman Wyden, Senator Allen, members of the Subcommittee on Science, Technology and Space, I appreciate the opportunity to submit testimony today on behalf of the Electronic Industries Alliance. I thank the Chairman for holding today's hearing on Internet security. There are few issues that are of more importance to the 2,300 member companies of EIA.

The Internet has become indispensable to the way we do business. The Internet empowers organizations to conduct e-commerce, provide better customer service, collaborate with partners, reduce communications costs, improve internal communication, and access information quickly.

In the rush to benefit from the Internet, organizations often overlook significant risks. For example, the engineering practices and technology used by many system providers do not produce systems that are immune to attack. Most network and system operators do not have the resources and technical expertise to defend attacks and minimize damage. Policy and law in cyberspace lag behind the pace of change. And lastly, security practices are underdeveloped, poorly disseminated and erratically followed.

For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated users can use them. Subsequently, serious attackers have a pool of technology they can use and mature to launch damaging attacks and to effectively disguise the source of their activities.

Attack technology is developing in an open source environment and is evolving rapidly. Technology experts and users are improving their ability to react to emerging problems, but we are behind. Significant damage to our systems and infrastructure can occur before effective defenses can be implemented. As long as our strategies are reactionary, this trend will worsen.

Our dependence on the Internet and the increased prevalence of attacks have created a true challenge for policymakers. As policymakers contemplate how to best protect the Internet and try to ascertain the proper role of government on the Internet, the reality remains: as a rule, technology has exponentially outpaced the establishment of sound policy.

As a result, it is incumbent upon the business community to take the lead in providing answers to Internet security. Similar to the Y2K crisis, only when our corporate boardrooms recognize their fiduciary responsibility to provide secure systems that Internet security will be addressed adequately.

Relatedly, the Electronics Industry Alliance recently formed the Internet Security Alliance (ISA) in conjunction with Carnegie Mellon University's CERT Coordination Center and a cross-sector of private companies including NASDAQ, Mellon Financial and AIG. The Alliance is an industry-led, global, cross-sector network focused on providing solutions to the challenges of the Internet economy. The mission of ISA is to bring Internet security to the forefront in corporate boardrooms worldwide.

Current Internet Security Policy

The control of U.S. cybercrime/cybersecurity policy has traditionally been viewed as an issue for the law enforcement and national defense communities—not an economic policy issue. Solutions have been expressed in terms of criminal sanctions, counter-terrorism efforts and law enforcement training rather than the prevention managed by the users of the information assets, like businesses and individuals.

However, law enforcement and national security communities do not have all the answers. In addition to leadership from private industry, the following goals need to be met in any national policy:

- A National strategy from the President after consultation with leadership of constituencies for coordinated responses to threats and attacks, like those developed for Y2K including:
  - Establishment of empowered organizations for sharing information about cyber-threats, attacks and remedies such as the Internet Security Alliance, the sectoral ISACs, and similar government and international groups
- Incentives for industrial and government institutions to adopt top-down policies of institutional security—including information technology/network security—that include:
  - Clear designation of responsibility/delegation from CEO
  - Creation of risk management plan
  - Investments in employee enculturation and user education
  - Establishment of best practices regarding high value/high risk environments in information technology, for example:
    - Establishment of organizational CIO
    - Employee education on IT security practices
    - Deployment of best practices technologies
      - Firewalls
      - Antiviral software
      - PKI authentication/encryption for e-mail/Internet
    - In government, necessary training and funding for these types of programs.

What we need to avoid in establishing a national policy:

New technology-specific criminal statutes that will result in the hobbling of vendor industries and slowing of deployment of leading edge technologies to the mass of internet users.

Where can the private sector help?

Organizations must search for an industry-led, global, cross-sector network focused on providing solutions to the challenges of the Internet Economy. We are at risk, and the business community must make it a leadership priority. The following are examples of what the private sector should be doing:

Information Sharing

Maintaining an adequate level of security in this dynamic environment is a challenge, especially with new vulnerabilities being discovered daily and attack technology evolving rapidly in an open-source environment. To help organizations stay current with vulnerabilities and emerging threats the private sector must concentrate on providing the following:

- **Vulnerability catalog:** a complete record of past vulnerability reports. New entries would be added to the catalog as they were reported.
- **Technical threat alerts:** in the form of "special communications" provide early warning of newly discovered security threats and are updated as analysis activities uncover additional information. Ranging from alerts on newly discovered packages of malicious code, such as viruses and trojan horses, to in-depth analysis reports of attack methods and tools, these reports would help organizations defend against new threats and associated attack technology.
- **Member information exchange:** augmenting the basic services listed above, an organization would have to develop an automated information sharing mechanism that allows business and individuals to anonymously report vulnerability, threat, and other security information that they are willing to share with other secure channels.
- **Threat analysis reports:** today the great majority of Internet security incidents are conducted by unknown perpetrators who act with unknown motivations to achieve unknown goals. Managing security risks in the long-term will

require a better understanding of the perpetrators and the economic, political and social issues that drive them.

Best Practices/Standards

Effective management of information security risks requires that organizations adopt a wide range of security practices. From basic physical security controls that prevent unauthorized access to computing hardware, to user-focused practices on password selection, to highly-detailed system administration practices focused on configuration and vulnerability management, these practices help organizations reduce their vulnerability to attacks from both outsiders and insiders.

- **Practices catalog:** beginning with existing practice collections and standards, and in collaboration with any participating companies an organization must develop a catalog of practices that span the full range of activities that must be addressed when developing an effective risk management program. The catalog will contain high-level descriptions of the required practices and should be made publicly available

Security Tools

While a sizeable commercial marketplace has developed for hardware and software tools that can be used to enhance an organization's security and a variety of tools can now be purchased, comprehensive tool sets are lacking. To fill the gaps, organizations build their own or find and evaluate public domain tools—a time consuming and expensive activity. An organization would have to establish a tools exchange: a restricted access repository where network administrators only can exchange special purpose tools they have created as well as information about, and evaluation of, public domain tools available over the Internet.

Policy Development

While there are many things an organization can do to enhance its security, some issues require broad action. For example, overall security could be improved through increased information sharing between industry and government, but FOIA *(Freedom Of Information Act)* regulations deter companies from sharing sensitive information with the government. Other issues like privacy and the proposed HIPPA legislation could also affect network security. An organization needs to identify these overarching issues and work with the appropriate industry and government organizations to advocate policy that effectively addresses the issues.

Other Critical Areas

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Enhanced incident response capabilities—The incident response community has handled most incidents well, but is now being strained beyond its capacity. In the future, we can expect to see multiple broad-based attacks launched at the Internet at the same time. With its limited resources, the response community will fragment, dividing its attention across the problems, thereby slowing progress on each incident.
- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.
- The problem is the fact that the demand for skilled system administrators far exceeds the supply.
- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.
- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer criminals is unlikely, and thus little deterrent value is realized.
- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. There is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a

"silver bullet" are lulled into a false sense of security and become less vigilant. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.

- There is little evidence of improvement in the security features of most products. Developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. Until their customers demand products that are more secure, the situation is unlikely to change.
- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

Summary

While it is important to react to crisis situations when they occur, it is just as important to recognize that information assurance is a long-term problem. The Internet and other forms of communication systems will continue to grow and interconnect.

- More and more people and organizations will conduct business and become otherwise dependent on these networks.
- More of these organizations and individuals will lack the detailed technical knowledge and skill that is required to effectively protect systems today.
- More attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain.
- The network and computer technology will evolve and the attack technology will evolve along with it.
- Many information assurance solutions that work today will not work tomorrow.

Managing the risks that come from this expanded use and dependence on information technology requires an evolving strategy that stays abreast of changes in technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks. To move forward, we will need to make improvements to existing capabilities as well as fundamental changes to the way technology is developed, packaged, and used.

Attacks will happen—they will become more sophisticated as our technology becomes more sophisticated. The best defense we can take as a nation is to ensure our networks and systems are properly fortified against them.

ARTICLE FROM NEWSWEEK BUSINESS INFORMATION, INC., NEWSBYTES

Brian McWilliams, July 21, 2001

A glitch in an ActiveX control shipped with Microsoft's Outlook e-mail program could enable an attacker to take full control of a victim's computer, Microsoft confirmed today.

The flaw, which affects all versions of Outlook, including Outlook 2002, which Microsoft bundles with its new Office XP suite, lies in an ActiveX program named "Microsoft Outlook View Control," according to Scott Culp, head of Microsoft's security response center.

By design, the affected ActiveX control allows Web pages to passively display to users the contents of their Outlook inbox. But a bug in the program could enable a specially designed Web page or HTML-based e-mail to run malicious programs on the victim's computer without permission.

The flaw, which was reported to the company Monday by security researcher Georgi Guninski, also could allow an attacker to read, modify, or delete e-mail in the victim's Outlook inbox, said Culp.

Guninski published an advisory on the bug today at his Web site titled "The more money I give to Microsoft, the more vulnerable my Windows computers are." Guninski also posted a harmless demonstration of the vulnerability, including source code.

Culp said Microsoft intends to release a bulletin about the flaw later today, and will follow with a patch as soon as possible. To protect against attacks in the meantime, the company advises Outlook users to disable ActiveX in the Internet Zone of Internet Explorer.

Outlook users who have applied the Outlook Security Update are not vulnerable to the e-mail based vector of attack, nor are Outlook 2002 users. But the flawed ActiveX control could still expose them to Web-based exploits, according to Culp.

While Guninski has uncovered dozens of security vulnerabilities in Microsoft's products including Internet Explorer, Outlook, Windows Media Player, Word, and Excel, the bug published today is the first he has found that affects Office XP, which Microsoft launched in May.

According to Guninski's advisory, Bulgarian native recently bought a copy of Office XP and discovered "it was quite unpleasant feeling giving so much money for so buggy product."

Microsoft's Culp told Newsbytes that by publishing the flaw before Microsoft had a patch ready, Guninski was only benefiting malicious hackers.

"Mr. Guninski is a poster child for bad behavior when it comes to responsible reporting practices. If your goal is to make the Internet more secure, you work with the vendor. Unfortunately, Mr. Guninski has put countless of customers at risk for no good reason," said Culp.

The Guninski advisory is at http://www.guninski.com/vv2xp.html.

Microsoft's security homepage is at http://www.microsoft.com/technet/itsolutions/security/default.asp.

Information on disabling ActiveX in Internet Explorer is at http://users.rcn.com/rms2000/acctroj/howto.htm.

Reported by Newsbytes, http://www.newsbytes.com.

○