IDENTITY THEFT: THE CAUSES, COSTS, CONSEQUENCES, AND POTENTIAL SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 22, 2004

Serial No. 108–272

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

98–486 PDF WASHINGTON : 2005

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

CONTENTS

IDENTITY THEFT: THE CAUSES, COSTS, CONSEQUENCES, AND POTENTIAL SOLUTIONS

WEDNESDAY, SEPTEMBER 22,

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:46 p.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Dan Daly, professional staff/deputy counsel; Juliana French, clerk; Adam Bordes, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good afternoon, and welcome to the subcommittee's hearing entitled, "Identity Theft: The Causes, Costs, Consequences, and Potential Solutions."

Today the subcommittee conducts its 11th hearing this Congress on cybersecurity issues, and this is the 39th hearing overall of this subcommittee in the 108th Congress. I certainly want to commend staff for the majority and staff for the minority and the hard work that they have put into all of these hearings and the work of the membership, as we have covered an awful lot of ground in this Congress.

Throughout the 108th Congress, the subcommittee has focused a great deal of attention and oversight on the topic of computer information security, and the growing cyberthreat to this Nation. This hearing will examine the cybersecurity threat from a somewhat different perspective and delve into an issue that has already adversely impacted millions of Americans and has the potential to become even worse as more and more information is gathered, stored and shared through the Internet in an all too often unprotected environment.

The issue is computer identity theft. I am concerned about the threat that identity theft poses to the U.S.' national and economic security. Identity theft is one of the fastest-growing crimes in the United States, and it appears that the battleground is expanding from one populated primarily by those seeking notoriety, to those seeking profit and disruptive impact. Federal statistics show that

nearly 10 million identities were stolen in the United States last year alone, and that the total cost of this crime in the United States is approximately $50 billion per year. Some predict that the worldwide costs of identity theft in all of its forms will exceed $2 trillion in financial losses by the end of 2005. These numbers are staggering, and they highlight why this hearing is so important.

As use of the Internet continues to expand every day, more personal information is converted into electronic data. Both the Federal Government and the private sector maintain large data bases of personal information about their employees and customers. The efficiencies realized through the increased availability of electronic data storage and transmission are tremendous, but the wealth of available personal information in digital form also provides a target-rich environment for criminals and terrorists. By hacking into data bases, paying off insiders, loading spyware onto users' machines or using fraudulent e-mails to trick users into revealing Social Security and other account numbers, criminals and terrorists are utilizing the Internet to profit illegally.

It seems as if not a day goes by without a new report of some worm, virus, phishing scheme or other cybercrime threatening users of the Internet. This week we have also learned that there is a dramatic increase in the number of zombie PCs, also called bots. These are computers infected by worms or Trojans and taken over surreptitiously by hackers and used to send spam, more viruses, harvest financial and personal information, or launch denial of service attacks. It is estimated that the number of computers being taken over by remote control is now averaging 30,000 per day, peaking at 75,000 in a single day. We need to quarantine and vaccinate infected computers, close the back doors, shut down the tunnels and cutoff bad guy access to our computers and networks.

A recent crackdown on cybercrime by the Department of Justice known as Operation Web Snare demonstrates just how large a problem cybercrime has become. The Department, through its U.S. Attorneys' offices, its Criminal Division, and the FBI, coordinated with the Secret Service, the FTC and a variety of other State, local and Federal and foreign law enforcement agencies, conducted this operation. Investigators identified more than 150,000 victims with estimated losses of more than $200 million. This operation to date has resulted in more than 150 arrests and convictions for electronic crimes including identity theft, fraud, counterfeiting software, computer intrusions and other intellectual property crimes.

We have representatives from the FBI, the FTC and the Secret Service with us here today. I applaud your efforts and the efforts of all of those involved in this operation, and I thank you for your service to this Nation.

In addition to highlighting the threat of organized crime on the Internet, Operation Web Snare touched on another growing problem: the potential nexus between cybercrime and terrorism. The report on the operation noted that terrorists and their support groups are hiding behind the cloak of the Internet to conceal their true locations and to communicate, generate funds and develop resources in support of terrorism. Furthermore, the report noted an increase in on-line complaints in which illegally obtained funds are flowing to parts of the world where terrorist groups are known to operate.

Operation Web Snare makes it clear that this is a global problem, and not only are criminals and terrorists aware of the vulnerabilities in cyberspace, but they are exploiting them for monetary profit as well. Make no mistake about it, our Nation's information systems are under attack 24 hours a day, 7 days a week from around the world. We cannot stick our heads in the sand and ignore these problems or continue to make excuses for why we are not taking more affirmative action. We have to address them head on and make sure that our cyberdefenses are prepared to repel these intruders.

Unfortunately through the work of this subcommittee, through our extensive research and oversight, I am not convinced that we are prepared either in the public or the private sector to adequately deal with these problems. I fear that cybercrime may get worse before it gets better. And I do not wish to wait for some large-scale failure of our Internet infrastructure or the launch of a combined physical and confined cyberattack against our citizens and our economy before we as a Nation get serious about protecting our information systems.

About a year ago, after several oversight hearings on the subject, in an information-gathering visit to Silicon Valley, I began to realize just how vulnerable this Nation had become to a growing and dangerous threat of cyberattack. Not only were Federal agencies failing to comply with the requirements of the law as outlined by FISMA, but the private sector was also seriously delinquent in its attention to these matters. After examining alternatives, we drafted the Corporate Information Security Accountability Act, which would have set forth certain computer information security plan reporting requirements for publicly traded companies in an effort to elevate the profile of this matter to the "C" level of management and respective boards of directors.

I did not introduce the legislation at that time, preferring a private-sector-driven, market-based solution to this growing threat to the American people and the economy, and hearing from the private sector that they could address this issue without the assistance or intervention by Congress. Well, here we are a year later, and, quite frankly, not only has the problem not gotten much better, there is compelling evidence, some of which we will hear today, that the problem was getting worse, and perhaps a lot worse. Thankfully, there are some key stakeholders such as Microsoft, RSA and AOL who are taking visible steps to proactively address this challenge.

But the world has grown to be a very dangerous place. Most of us make sure that we lock our doors and windows in our homes and businesses before we end the day. Some even pay extra to have an alarm system installed in their home or business to provide protection against unwanted intruders who wish to do us harm or steal our assets. In today's digital world, we must also protect our cyberassets and our personal information from intruders, both internal and external, from those who would do us harm and steal our information.

We have not focused sufficiently on this challenge, and as a result our personal and national security, and our personal and national economic stability, are subject to a growing risk from en-

emies who may attack at any time of day and night from anywhere in the world 365 days a year.

So today I call on this Nation, everyone in this Nation, to take immediate actions to increase their protection and to dramatically improve the cybersecurity profile of this country. We are all stakeholders, and we all have responsibility to be a part of the solution and not a continuing part of the problem.

I call on major corporations to schedule on the agenda of their next senior management meeting and their next board of directors meeting, a discussion about your company's computer information security plan. This is a management, governance and business process issue and must be treated accordingly. Have you invested in the implementation of fundamental information security best practices and benchmarks, and is your IT security risk assessment and risk management plan up to date? The National Cybersecurity Partnership, with the tremendous help and leadership of the Business Software Alliance and others, has produced a Guide to Corporate Governance that provides tools and strategies that corporations can affordably implement immediately.

I am tired of hearing that lawyers are advising against the adoption and implementation of cybersecurity best practices or on-line privacy policy because they are afraid that they may be creating liability. Friends, in my estimation, a failure to aggressively address these issues may in and of itself be creating the liability. While I am not a lawyer, I am a businessman, I am a citrus grower, taxpayer, I am an involved citizen. This issue is about national security and economic stability along with sound business practices and deserves immediate attention. How about training for employees and information about how to protect their home computers from unwanted intruders and thieves? What a great and inexpensive corporate benefit that would be. And for those who are already doing that, thank you, and keep up the great work.

We call on the larger businesses of corporate America to work with your entire supply chain to demand that all the businesses that connect to your network understand the responsibility to make sure their systems are secure.

We speak to the financial services sector, credit card companies, health care providers and others to reexamine their own information security protection profiles. Many Americans trust you with their most personal information and have an expectation that the information will remain confidential and protected.

Why are we experiencing such a proliferation of identity theft? Is the day of the pin and password behind us, and we need to move immediately to a two-part authentication process that may include biometrics? Are we making the necessary investments to protect the information? Or do some view the cost of identity theft as merely the cost of doing business?

I call on software and hardware manufacturers and the national associations that represent you to take the lead from a number of major CEOs who have already publicly committed to improving the quality and security of their products by issuing a public statement that makes that commitment in a manner that the public can have the confidence to know that you, too, view the proliferation of worms, viruses and other challenges resulting from vulnerabilities

in your software and hardware products as a matter deserving of a greater investment of time and resources to provide sturdier and more secure products for the marketplace.

I would further call on those same hardware and software manufacturers to expand your commitment to providing the consuming public with secure out-of-the-box computing products with user-friendly instructions, preset default security controls, and alerts about creating and maintaining a secure computing environment.

I call on the manufacturers of these essential products to work more closely with critical infrastructure sectors to provide security and configuration requirements in advance and build those requirements into the life cycle development process to deliver more compatible, secure and higher-quality products to the marketplace. Companies like Oracle, Microsoft, Sun, Verizon and Entrust are examples of those who are taking this matter seriously.

I call on Internet service providers and operating systems manufacturers to work more aggressively with other public and private stakeholders to provide consumers of all levels of sophistication—to provide information about affordable, user-friendly tools that are available to help protect themselves and immediately improve their cybersecurity hygiene.

We urge small businesses to take the time and learn about steps that you can take that are affordable and user-friendly to make your system more secure from the growing threats of cyberspace. There are fundamental steps in cybersecurity hygiene that will improve your protection profile overnight.

You are an important stakeholder in this matter, and you have a responsibility to be a part of the solution. Home users are not exempt. Home users can become more aware of the tools that are available to improve the protection of their home computer. Make sure that you know about the antivirus software and personal firewalls and how to update your applications, including your operating system, in a timely manner.

The National Cybersecurity Alliance is sponsoring National Cybersecurity Awareness Month during October, and you may get a lot of the necessary information about fundamental steps that you can take to protect yourselves by visiting their Website at www.staysafeonline.info.

Today we call on the States and local governments to examine their own information security plans, along with their education, awareness and training programs, and, again, to speak to the agencies of the Federal Government, large and small, to step up and provide the example for the rest of the Nation. Receiving Ds and Fs on scorecards about requirements and compliance with the law is unacceptable. We must absolutely experience a recommitment by every Cabinet Secretary, department agency and bureau head to address the issue of securing the Federal computer networks and protecting the information assets that they contain. Federal CIOs and CISOs must be empowered to develop and implement effective strategies and to examine opportunities for enterprise solutions.

And we call on Congress to work with all stakeholders, including military, intelligence and law enforcement agencies, domestic and international, to ensure an adequate level of preparedness to meet

this growing cyberchallenge and recognize this battle in an overall threat domain.

There is much that each of us can do today. The magnitude of this threat demands that we pay increased attention to the issue. If each of us takes the steps today to ensure that we have implemented the basic fundamental elements of cybersecurity hygiene, the cybersecurity protection profile of this Nation will improve overnight. We will send in an enormous message to all of the bad guys that we take this challenge seriously, and we will make the necessary steps to protect our national security and economic stability.

As e-government, e-commerce, e-banking and e-health continue to take hold, we must be sure that we have a comprehensive national strategy that provides flexibility, while encouraging innovation and creativity in developing the tools and strategies necessary to secure the computer networks of this Nation and to protect the information that they contain.

Today's hearing provides the subcommittee the opportunity to examine this challenge in the context of the impact that unprotected computers and networks have had on the rise of computer-related identity thefts and the adverse impact that these data thefts are having on the national security and economic profile of this Nation.

We will hear from experts about potential solutions to these problems, such as vulnerability management, credentialing and authentication tools which may help reduce the impacts of viruses, worms, spyware, spam and phishing, and in return reduce identity-related cyberthefts.

I eagerly look forward to the expert testimony that our panel of leaders in information security will provide today, as well as the opportunity to discuss the challenges ahead. Today's hearing can be viewed live via Webcast by going to reform.house.gov and clicking on the multimedia link.

[The prepared statement of Hon. Adam H. Putnam follows:]

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
CONGRESSMAN ADAM PUTNAM, CHAIRMAN

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: ***"Identity Theft: The Causes, Costs, Consequences, and Potential Solutions"***

Wednesday, September 22, 2004
2:45 p.m.
Room 2154, Rayburn House Office Building

OPENING STATEMENT

Good afternoon and welcome to the Subcommittee's hearing entitled - "Identity Theft: The Causes, Costs, Consequences, and Potential Solutions." Today, the Subcommittee conducts its eleventh hearing this Congress on cyber security issues. Throughout the 108th Congress, the Subcommittee has focused a great deal of attention and oversight on the topic of computer information security and the growing cyber threat to this nation. This hearing will examine the cyber security threat from a somewhat different perspective, and delve into an issue that has already adversely impacted millions of Americans and has the potential to become even worse as more and more information is gathered, stored and shared through the Internet in an all-to-often unprotected environment. That issue is computer identity theft. I am concerned about the threat that identity theft poses to the United States' national and economic security. Identity theft is

one of the fastest growing crimes in the United States and it appears that the battleground is expanding from one populated primarily by those seeking notoriety...to those seeking profit and disruptive impact. Federal statistics show that nearly 10 million identities were stolen in the United States last year, and that the total cost of this crime in the United States is approximately $50 billion dollars a year. Some predict that the worldwide costs of identity theft in all of its forms will exceed $2 trillion in financial losses by the end of 2005. Those numbers are staggering, and they highlight why this hearing is so important.

As use of the Internet continues to expand, everyday more personal information is converted into electronic data. Both the Federal government and the private sector maintain large databases of personal information about their employees and customers. The efficiencies realized through the increased availability of electronic data storage and transmission are tremendous. However, the wealth of available personal information in digital form also provides a target-rich environment for criminals and terrorists. By hacking into databases, paying off trusted insiders, loading spyware on to users' machines, or using fraudulent e-mails to trick users into revealing Social Security and other account numbers, criminals and terrorists are utilizing the Internet to illegally profit.

It seems as if not a day goes by without a new report of some worm, virus, phishing scheme, or other cyber crime threatening users of the Internet. This week, we have also learned that there is a dramatic increase in the number of zombie PCs. Also called "Bots", these are computers infected by worms or Trojans and taken over surreptitiously by hackers and used to send spam, more viruses, harvest financial and personal information, or launch denial of service attacks. It is estimated that the number of computers being taken over by remote control is now averaging 30,000 a day, peaking at 75,000 in a single day. We need to quarantine and "vaccinate" infected computers, close the back doors, shut down the tunnels, and cut off "bad guy" access to our computers and networks.

A recent crack down on cyber crime by the Department of Justice, known as Operation Web Snare, demonstrates just how large a problem cyber crime has become. The Department through its U.S. Attorneys' offices, its Criminal Division, and the FBI, coordinated with the Secret Service, the FTC, and a variety of other federal, state, local, and foreign law enforcement agencies to conduct this operation. Investigators identified more than 150,000 victims with estimated losses of more than $215 million dollars. This operation to date has resulted in more than 150 arrests and convictions for electronic crimes including identity theft, fraud, counterfeiting software, computer intrusions, and other intellectual property crimes. We have representatives from the FBI, the FTC, and the Secret Service with us here today. I applaud your efforts and the efforts of all of those involved in this operation, and I thank you for your service to this nation.

In addition to highlighting the threat of organized crime on the Internet, Operation Web Snare touched on another growing problem, the potential nexus between cyber crime and terrorism. The report on the operation noted that terrorists and their support groups are hiding behind the cloak of the Internet to conceal their true locations and to communicate, generate funds, and develop resources in support of terrorism.

Furthermore, the report noted an increase in online complaints in which illegally obtained funds are flowing to parts of the world where terrorist groups are known to operate. Operation Web Snare makes it clear that this is a global problem and not only are criminals and terrorists aware of the vulnerabilities in cyber space, but they are exploiting them for monetary profit as well.

Make no mistake about it. Our nation's information systems are under attack 24 hours a day, 7 days a week from all across the world. We cannot stick our heads in the sand and ignore these problems or continue to make excuses for why we are not taking more affirmative action. We have to address them head on and make sure that our cyber defenses are ready to repel these intruders. Unfortunately, through my extensive research and oversight, I am not convinced that we are prepared either in the public or private sector to adequately deal with these problems. I fear that cyber crime may get worse before it gets better, and I do not wish to wait for some large scale failure of our Internet infrastructure...or the launch of a combined physical and cyber attack against our citizens and our economy... before we as a nation get serious about protecting our information systems.

About a year ago, after several oversight hearings on this subject, and an information gathering visit to Silicon Valley, I began to realize just how vulnerable this nation had become to a growing and dangerous threat of cyber attack. Not only were federal agencies failing to comply with the requirements of the law, as outlined by the Federal Information Security Management Act (FISMA), but the private sector was also seriously delinquent in its attention to these matters.

After examining a number of alternatives, I drafted the Corporate Information Security Accountability Act (CISAA), which would have set forth certain computer information security plan reporting requirements for publicly traded companies, in an effort to elevate the profile of this matter to the "C" level of management and respective Boards of Directors. I did not introduce the legislation at that time, preferring a private-sector driven market based solution to this growing threat to the American people and the U. S. economy, and hearing from the private sector that they could address this issue without the assistance or intervention by Congress.

Well folks...here we are a year later, and quite frankly, not only has this problem not gotten much better, there is compelling evidence...and we will hear some of it today...that this problem is getting worse...and maybe a lot worse. Thankfully, there are some key stakeholders such as Microsoft, RSA, and AOL who are taking visible steps to proactively address this critical challenge.

Unfortunately, the world has grown to be a very dangerous place. Most of us make sure that we lock our doors and windows in our homes and businesses before we end the day. Some even pay extra to have an alarm system installed in their home or business to provide extra protection against unwanted intruders who may wish to do us harm or steal our assets.

In today's digital world, we must also protect our cyber assets and our personal information from intruders...both internal and external...from those who would do us harm or steal our assets. We have not focused sufficiently on this challenge and as a result... our personal and national security AND our personal and national economic stability are subject to a growing risk...from enemies who may attack at any time of day or night, from anywhere in the world, 365 days a year.

Accordingly, on this day and at this time...I am calling on this nation...everyone in this nation...to take immediate actions to increase your protection and to dramatically improve the cyber security profile of this nation...TODAY! We are ALL stakeholders, and we ALL have a responsibility to be a part of the solution...and not a continuing part of the problem.

I call on major corporations to schedule on the agenda of your NEXT senior management meeting AND your next Board of Directors meeting, a discussion about your company's computer information security plan. This is a management, governance and business process issue and must be treated accordingly. Have you invested in the implementation of fundamental information security "best practices" and benchmarks and is your IT security risk assessment and risk management plan up-to-date? The National Cyber Security Partnership, with the great help and leadership of the Business Software Alliance and others, has produced a Guide to Corporate Governance that provides tools and strategies that corporations can affordably implement immediately. I am simply tired of hearing that lawyers are advising against the adoption and implementation of cyber security best practices or online privacy policies because they are afraid that they may be creating liability. My friends...in my estimation, a failure to aggressively address these issues may in and of itself be creating that liability. While I am not a lawyer, I am a businessman...I am a taxpayer...and I am an involved citizen. This issue is about national security and economic stability along with sound business practices and deserves your immediate attention.

How about training for employees and information about how to protect their home computers from unwanted intruders and thieves? What a great...and inexpensive corporate benefit that would be...and for those who are already doing that...thank you and keep up the great work!

I call on the larger businesses of corporate America to work with your entire supply chain to demand that all of the businesses that connect to your network understand their responsibility to make sure that their systems are secure.

I call on the financial services sector, credit card companies, health care providers, and others to re-examine their own information security protection profiles. Many Americans trust you with their personal information and have an expectation that the information will remain confidential and protected. Why are we experiencing such a proliferation of identity theft? Is the day of the pin and password behind us and we need to move immediately to a two-part authentication process that may include some type of

biometric? Are we making the necessary investments to protect the information or do some view the cost of identity theft as just a "cost of doing business"?

I call on software and hardware manufacturers and the national associations that represent you to take the lead from a number of major CEO's who have already publicly committed to improving the quality and security of their products, by issuing a public statement that makes that commitment in a manner that the consuming public can have the confidence to know that you, too, view the proliferation of worms, viruses and other challenges resulting from "vulnerabilities" in software and hardware products as a matter deserving of a greater investment of time and resources to provide "sturdier" and more secure products to the marketplace. I further call on those same software and hardware manufacturers to expand your commitment to providing the consuming public with secure "out-of-the-box" computing products with user-friendly instructions, pre-set "default" security controls, and alerts about creating and maintaining a secure computing environment. I also call on the manufacturers of these essential products to work more closely with critical infrastructure sectors to identify security and configuration requirements in advance and build those requirements into the life cycle development process to deliver more compatible, secure and higher quality products to the marketplace. Companies like Oracle, Microsoft, Sun, Verisign and Entrust are examples of those who are taking this matter seriously.

I call on Internet Service Providers and Operating Systems manufacturers to work more aggressively with other public and private stakeholders to provide consumers of all levels of sophistication with information about affordable and user-friendly tools that are available to help them protect themselves and immediately improve their cyber security hygiene.

I call on all small business owners to take the time and learn about steps that you can take that are affordable and user-friendly to make your system more secure from the growing threats of cyber space. There are fundamental steps in cyber security hygiene that will improve your protection profile overnight. You are an important stakeholder in this matter and you have a responsibility to contribute to the solution.

I call on home users to become more aware of the tools that are available to you to improve on the protection of your home computer. Make sure you know about anti-virus software, and personal firewalls, and how to update to your applications, including your operating system, in a timely manner.

The National Cyber Security Alliance is sponsoring National Cyber Security Awareness Month during October and you may get a lot of the necessary information about fundamental steps that you can take to protect yourselves by visiting their website, www.staysafeonline.info.

Today I call on all states and local governments to examine their own information security plans, along with their education, awareness and training programs.

Additionally, today, I again call on the agencies of the federal government...big and small...to step up and provide the example for the rest of this nation. Receiving "D's" and "F's" on scorecards about your compliance with the requirements of the law is completely unacceptable. We absolutely must experience a re-commitment by every Cabinet Secretary, Department, Agency and Bureau Head...to address the issue of securing the federal computer networks and protecting the information assets that they contain. Federal CIO's and CISO's must be empowered to develop and implement effective strategies and to examine opportunities for enterprise solutions.

And lastly, today I again call on Congress to work with all stakeholders, including military, intelligence and law enforcement agencies...domestic and international...to ensure an adequate level of preparedness to meet this growing cyber challenge and to recognize this battle front in the overall threat domain.

Bottom line folks...is that there is much that each of us can do...TODAY! The magnitude of this threat demands that we pay increased attention to this issue. If each of us would take the steps today to insure that we have implemented the basic fundamental elements of cyber security hygiene...the cyber security protection profile of this nation will improve dramatically overnight we will send an enormous message to all of the bad guys that we take this challenge seriously and we will take the necessary steps to protect our national security and economic stability.

As e-government, e-commerce, e-banking, and e-health continue to take hold, we must be sure that we have a comprehensive national strategy that provides flexibility, while encouraging innovation and creativity in developing the tools and strategies necessary to secure the computer networks of this nation and protect the information assets that they contain.

Today's hearing will provide the Subcommittee the opportunity to examine this growing challenge in the context of the impact that unprotected or inadequately protected computers and networks have had on the rise of computer related identity thefts, and the adverse impact that these data thefts are having on the national security and economic stability of this nation. We will hear from experts about potential solutions to these problems, such as vulnerability management, credentialing and authentication tools, which may help reduce the impact of viruses, worms, spyware, spam, and phishing and in turn reduce identity related cyber thefts.

I eagerly look forward to the expert testimony that our distinguished panel of leaders in information security will provide today as well as the opportunity to discuss the challenges that lie ahead.

Mr. PUTNAM. At this time I would like to recognize the distinguished ranking member of the subcommittee, the gentleman from Missouri Mr. Clay, for his opening statement.

Mr. CLAY. Thank you, Mr. Chairman for holding today's hearing for what is a new topic for our subcommittee, but also part of a growing threat to our Nation's economy, identity theft. That said, I am hopeful that our distinguished panelists will offer constructive and thoughtful proposals on how the Federal Government can be a catalyst for protecting its citizens from those using the Internet or other electronic methods for criminal activity.

The costs associated with identity theft activities are staggering when accounting for both economic losses and the time dedicated by victims to remedying credit ratings and financial records. According to the FTC September 2003 survey, the personal costs accumulated by victims of identity theft totals approximately $5 billion annually, with the average costs ranking between $500 and $1,200 per victim. In addition, approximately 15 percent of those surveyed had their personal information misused in nonfinancial activities, often subjecting them to legal investigations or other unwarranted personal invasions.

Although the Federal Government has taken steps to counter identity theft-related activity, I remain troubled that identity-theft related investigations are not properly coordinated among local, State and Federal agencies. While progress has been made in coordinating such investigations through the FTC's Identity Theft Data Clearinghouse, efforts must continue to ensure its interconnectivity to all State and local law enforcement jurisdictions. Success can only be achieved when such systems are seamless and interoperable with all stakeholders.

In closing, I am hopeful that this issue will remind us of the importance of ensuring the security of our Nation's critical infrastructure and the electronic commerce-based industry. Our Nation's security depends on it. Thank you, Mr. Chairman, and I yield back.

Mr. PUTNAM. I thank the gentleman.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

Statement of the Honorable Wm. Lacy Clay
Hearing on Identity Theft
September 22, 2004

Thank you, Mr. Chairman, for holding today's hearing on what is a new topic to our subcommittee, but part of a growing threat to our nation's economy—Identity Theft. That said, I am hopeful that our distinguished panelists will offer constructive and thoughtful proposals on how the federal government can be a catalyst for protecting its citizens from those using the Internet or other electronic methods for criminal activity.

The costs associated with identity theft activities are staggering when accounting for both economic losses and the time dedicated by victims to remedying credit ratings and financial records. According to the FTC's September 2003 survey, the personal costs accumulated by victims of identity theft totals approximately $5 billion annually, with the average cost ranging between $500 and $1,200 per victim. In addition, approximately 15% of those surveyed had their personal information misused in non-financial activities, often subjecting them to legal investigations or other unwarranted personal invasions.

Although the federal government has taken steps to counter identity theft related activities, I remain troubled that identity theft related investigations are not properly coordinated among local, state, and federal

agencies. While progress has been made in coordinating such investigations through the FTC's Identity Theft Data Clearinghouse, efforts must continue to ensure its interconnectivity to all state and local law enforcement jurisdictions. Success can only be achieved when such systems are seamless and interoperable with all stakeholders.

In closing, I'm hopeful that this issue will remind us of the importance of ensuring the security of our nation's critical infrastructure and electronic commerce based industries. Our nation's security depends on it.

Thank you, Mr. Chairman, and I yield back.

Mr. PUTNAM. And we will move right to testimony. I would ask the first panel of witnesses, and anyone accompanying you who will be providing support to your answers, to please rise and raise your right hands for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. I note for the record that all of the witnesses responded in the affirmative.

I would like to introduce our first witness for his opening statement. All of your written testimony will be included for the record. We would ask you to summarize those statements to a 5-minute opening, and we will begin with Mr. Swindle.

Commissioner Orson Swindle was sworn in as a Commissioner on the Federal Trade Commission in December 1977. Commissioner Swindle was appointed in December 2001 as head of the U.S. delegation to the Organization for Economic Cooperation and Development experts group to review the 1992 OECD guidelines for the security of information systems. Commissioner Swindle has had a distinguished military career and served in the Reagan administration from 1981 to 1989 directing financial assistance programs to economically distressed rural and municipal areas of the country.

We welcome you back to the subcommittee, sir, and you are recognized for 5 minutes.

STATEMENTS OF ORSON SWINDLE, COMMISSIONER, FEDERAL TRADE COMMISSION; STEVEN MARTINEZ, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION; LARRY JOHNSON, SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE; AND PATRICK O'CARROLL, ACTING INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION

Mr. SWINDLE. Thank you. Mr. Chairman, Mr. Clay and members of the subcommittee, I appreciate this opportunity to discuss the theft and misuse of electronic data and the FTC's efforts to promote better information security practices. My written statement represents the views of the Commission. My comments today are my own and do not necessarily reflect those of the Commission.

Consumers and businesses enjoy many benefits in today's information economy. We can purchase products, process financial transactions and access information at any time. The same information-rich data bases that make this possible also are attractive targets for identity thieves and other criminals. The challenge for each of us, consumers, businesses and government alike, is to protect these data bases and the national information infrastructure that supports them.

Vulnerabilities and threats to the information economy are very real. Many instances have occurred in which computers are stolen, our networks penetrated, and sensitive personal information of thousands of individuals compromised. These breaches of information security lead to identity theft and impose great cost on both consumers and businesses. Perhaps more damaging is the loss of consumer confidence in using electronic commerce and the vast benefits of the information age.

Addressing these threats begins with education. Consumers and businesses must learn how to better protect personal information. Law enforcement actions by the Federal Trade Commission and others can help stop harmful practices and highlight the importance of information security. We also encourage the development of authentication and other security technology to help protect consumers from spam and phishing attacks. This November the FTC will host a workshop to explore and promote the adoption of e-mail authentication standards.

Improving information security is essential to our society. We have conducted security-related workshops, worked with the OECD on its information security guidelines, issued the Gramm-Leach-Bliley Safeguards Rule, and brought numerous law enforcement actions. Some basic lessons are evident from our work.

First, information security is an ongoing, never-ending process of assessing risks and vulnerabilities. As security threats and technologies constantly evolve, so must our security measures.

Second, there is no one-size-fits-all solution for all organizations and types of information. Security procedures must be reasonable and appropriate with regard to the organization, the complexity and sensitivity of the information itself, and the nature and scope of activities in which the information is used.

Third, there is no such thing as perfect security. Breaches can happen, even when a company or person has taken every reasonable precaution. Conversely, the absence of a breach does not necessarily mean that adequate security precautions are in place.

Fourth, all computer users have an extraordinary role to play in achieving adequate information security, and they must do their job. Information security demands that all of us be involved.

Recognizing these lessons, we believe there are some basic steps businesses can take to help minimize vulnerabilities and compromises. Businesses should implement a security plan and make good information practices an essential part of their business operations, literally a part of their business culture. Information security practices must include: risk assessment; identifying internal vulnerabilities and external threats to personal information; designing and implementing safeguards to control these risks; routinely evaluating effectiveness of these safeguards; adjusting the plan as necessary to maintain effective security; and overseeing the information-handling practices of third-party or affiliated service providers who have access to personal information.

A good security plan includes effective response procedures should a breach or compromise of sensitive personal information occur. For example, if the breach would result in harm to a person or business, report the situation to appropriate law enforcement agencies. If a breach affects other businesses, such as when a company stores personal information on behalf of other businesses, notify that business.

In addition, some breaches dictate that businesses notify customers. Although notifying customers or consumers may not be necessary in all situations, when identity theft is possible because of a breach, customers need to know this quickly. For example, the theft of Social Security numbers. Early notification of consumers allows them to take steps to limit harm, such as placing a fraud

alert on their credit file with a consumer reporting agency. The FTC provides businesses valuable information and advice on steps to take in the event of an information security breach.

Our law enforcement and education efforts should help deter identity theft before it occurs. However, identity theft will no doubt continue, and the FTC has a comprehensive program to assist consumers and businesses who become victims.

The Commission serves as the Federal Government's central repository for identity theft complaints. We take the lead in referring complaints about identity theft to appropriate law enforcement authorities. We provide victim assistance and consumer education. Our identity theft Website provides a variety of resources for both customers and businesses.

Educating customers and businesses about the risks to personal information and the importance of good security practices has high priority at the Commission. We will pursue those who violate information security laws, and we will provide assistance to victims of identity theft.

Chairman Putnam, in closing I would like to thank you and Chairman Davis for your Dear Colleague letters in support of the National Cybersecurity Awareness Month and your personal leadership on these issues in general. Thank you for this opportunity today, and I look forward to responding to your questions.

Mr. PUTNAM. Thank you very much, Commissioner.

[The prepared statement of Mr. Swindle follows:]

PREPARED STATEMENT OF THE
FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

on

PROTECTING INFORMATION SECURITY AND PREVENTING IDENTITY THEFT

September 22, 2004

I. INTRODUCTION

Mr. Chairman, and members of the subcommittee, I am Commissioner Orson Swindle.[1] I appreciate the opportunity to appear before you today to discuss the Commission's role in promoting information security and combating identity theft.

The Federal Trade Commission has a broad mandate to protect consumers from unfair and deceptive practices. As part of its mission, the Commission has given a special emphasis to efforts to protect the privacy and security of consumer information. These efforts include educating companies about the importance of using reasonable and appropriate procedures to safeguard consumers' personal information, supplemented by law enforcement in appropriate cases when companies fail to take such steps. In addition, as the federal government's central repository for identity theft complaints, the Commission plays a significant role in referring complaints about identity theft to appropriate law enforcement authorities, providing victim assistance and consumer education, and working with businesses to mitigate harm in the event of a security breach.[2]

II. THE BENEFITS AND RISKS OF ELECTRONICALLY-STORED CONSUMER DATA

Electronic information systems provide enormous benefits to consumers, businesses, and government alike. We rely on them for the orderly operation of our financial systems and power supplies, the efficient processing of our transactions, twenty-four hour access to information, and many other conveniences and cost savings. In order to provide these benefits, these computer-driven systems store voluminous data on consumers – ranging from sensitive medical and financial records to catalog purchases. If not adequately protected, these systems and databases

can be extremely vulnerable, thus threatening the security of the information they store and maintain.

In particular, a large database containing sensitive personal information can be a treasure trove for identity thieves.[3] When breached, the data in these systems can be used to impersonate consumers, take over their accounts, and cause substantial injury to consumers, businesses, and other institutions.[4] In recent years, there have been reports of a number of large-scale computer security breaches in which identity thieves and others gained access to the sensitive personal information of tens of thousands of consumers. Examples of publicly reported breaches include the theft of computer equipment containing detailed health insurance or financial information, security breaches that exposed credit card data, and the hacking of university databases. Breaches such as these create the potential for – and sometimes result in – mass-scale identity theft with millions of dollars in false charges.

Electronic systems and databases face diverse security threats. Sometimes, companies simply fail to properly safeguard consumers' information, leaving it vulnerable to hackers. Other breaches are caused by insiders, who exploit security weaknesses or use their position and access to the company's systems to steal data. In some instances, the breach can be as simple as the failure to dispose of sensitive documents properly. The adverse consequences of poor security can include not only identity theft and fraud, but also diminished computer operation, spam, "phishing" attacks, or even the takeover of computers to launch attacks on other commercial websites or on parts of the nation's critical information infrastructure.

III. PREVENTING BREACHES AND IDENTITY THEFT

Companies that process or store personal information about consumers – especially

sensitive information such as a Social Security number or credit card information – have a responsibility to safeguard that data. The Commission actively attempts to educate businesses and consumers about information security risks and the precautions they must take to protect or minimize risks to personal information. Our emphasis is on preventing breaches before they happen by encouraging businesses and consumers to make security part of their daily routines. We also provide advice to businesses and consumers in the event that a breach involving sensitive personal information does occur.

A. Reasonable Security Procedures

The Commission has considerable experience in understanding and addressing information security concerns. For example, in 1999, the Commission convened an Advisory Committee on Online Access and Security, in which a panel of experts examined the parameters of appropriate security for information collected online and provided a report with its findings.[5] The Commission also drafted and enforces its Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule"), which became effective in 2003.[6] This Rule requires "financial institutions" subject to the FTC's jurisdiction, which includes a broadly-defined group of non-bank entities, to develop and implement appropriate safeguards to protect customer information. In addition, the Commission played a leading role in developing and implementing the Organization for Economic Cooperation and Development's ("OECD") Security Guidelines.[7]

Through this work, as well as our more general education and enforcement initiatives, the Commission has come to recognize several principles that should govern any information security program. First, information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and

technology constantly evolve. Second, a company's security procedures must be reasonable and appropriate in light of the circumstances. Such circumstances include the company's size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles. Third, the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. Finally, a company's practices may be unreasonable even without a known breach of security. Indeed, because the primary purpose of information security is to prevent breaches before they happen, companies cannot simply wait for a breach to occur before they take action.

Implementation of these principles requires businesses to develop a security plan and make security monitoring and oversight part of their regular operations – literally, a part of their culture. Information security planning should include: identifying internal and external risks to the security, confidentiality, and integrity of consumers' personal information; designing and implementing safeguards to control these risks; periodically monitoring and testing the safeguards to be sure they are working effectively; adjusting security plans according to the results of testing or changes in circumstances; and overseeing the information handling practices of service providers who have access to the personal information. As discussed below, these basic steps are required by the Commission's Safeguards Rule and the Commission's orders in cases involving information security.

B. Managing a Data Compromise

Companies should implement reasonable security procedures to prevent the compromise of sensitive personal information. In the event that a security breach does occur, however, there

are several steps businesses should take to respond.[8]

For example, if the security breach could result in harm to a person or business, companies should report the situation to the appropriate law enforcement agency. Companies should also consider whether the data compromise may affect other businesses, and if so, should notify them. In particular, if a breach affects information that a company stores or maintains on behalf of another business, notification to the other business would be appropriate.

In addition, companies should evaluate whether to notify consumers that there has been a breach.[9] For example, consumer notification may not be necessary if the information is not sensitive or there is no evidence of unauthorized access. If information that creates a risk of identity theft has been stolen, however, the FTC suggests notifying individuals of the incident as soon as possible so they can take steps to limit the potential damage.[10] For example, if an individual's Social Security number is compromised, that individual, by placing a fraud alert on his credit file, will have a good chance of preventing, or at least reducing, the likelihood of identity theft or the misuse of this information.[11]

IV. THE FEDERAL TRADE COMMISSION'S INITIATIVES

The Commission seeks to highlight the importance of information security using several approaches, including educating consumers and businesses, targeted law enforcement actions, international cooperation, and encouraging the private sector to develop and deploy information security technologies. Pursuant to its mandate under the Identity Theft Act, the Commission also facilitates information sharing among public and private entities to combat and help prevent identity theft.[12] Further, the Commission is currently working on a number of rulemakings implementing provisions of the Fair and Accurate Credit Transactions of 2003 ("FACT Act")

that contain new and important measures to help reduce identity theft and facilitate identity theft victims' recovery.[13]

A. Education and Outreach

Education is an essential element of the Commission's information security efforts. Our educational initiatives include public workshops to highlight emerging issues, consumer and business education to help identify risks to personal information and promote a "Culture of Security," and business education to promote compliance with relevant laws. For example, last year we held a two-session workshop, "Technologies for Protecting Personal Information: The Consumer and Business Experiences," to educate businesses, consumers, and ourselves about the challenges and possible technological solutions to securing electronic data.[14] In order to secure systems that contain personal information, panelists advised that businesses adopt a comprehensive risk-management strategy that incorporates four critical elements: people, policy, process, and technology.[15] Panelists also discussed a variety of recent initiatives in which industry is applying these principles. For example, companies have worked to reduce security flaws in software code, ship products in a more secure configuration, add new security features to products, and provide better security support, such as providing warnings and security patches, to their already-deployed products when security flaws appear.[16] In addition, panelists explored identity management tools and authentication issues as part of a risk-management plan.[17]

Our information security campaign also includes extensive outreach to businesses and consumers through our website, educational alerts, speeches, and participation in joint cybersecurity initiatives with other government agencies and private groups. The Commission devotes a portion of its website to educating businesses and consumers about security, and these

security-related pages are some of the most popular on our site.[18] The site includes guidance for businesses to reduce risks to their computer systems,[19] and tips for consumers on selecting online security products.[20] Our recent outreach efforts have also included cooperative ventures with the Department of Homeland Security and such organizations as the National Cyber Security Partnership and the National Cyber Security Alliance Stay Safe Online.[21]

B. Law Enforcement

The Commission's enforcement tools in information security matters derive generally from Section 5 of the FTC Act[22] and the Commission's Safeguards Rule.

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[23] To date, the Commission's security cases have been based on its authority to prevent deceptive practices.[24] These cases involved companies that made alleged express or implied promises that they would take appropriate steps to protect sensitive information obtained from consumers, but did not do so.[25] The complaints and consent orders in these cases reflect the principles discussed in Section III.A., above, and provide guidance to industry about implementing reasonable security procedures. In particular, the orders require, among other things, that the companies establish and maintain a comprehensive information security program that includes the basic elements necessary to ensure reasonable and appropriate security.

The Commission also has responsibility for enforcing its Safeguards Rule. The Rule requires a wide variety of non-bank financial institutions to implement comprehensive protections for customer information.[26] The Commission has issued guidance on the Rule[27] and met with a variety of trade associations and companies to promote compliance. Currently, Commission staff is conducting non-public investigations of compliance with the Rule.

Finally, an effective security program includes measures to ensure proper disposal of sensitive consumer information once it is no longer needed. Pursuant to the recently enacted FACT Act,[28] the Commission issued a proposed rule designed to reduce the risk of fraud or identity theft by ensuring that consumer reports, or information derived from consumer reports, are appropriately redacted or destroyed before being discarded.[29] The Commission anticipates the issuance of a final rule by the end of the year. Once the rule is in effect, it will provide an additional tool for use in the Commission's law enforcement efforts.

C. International Cooperation

In an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information, and the Commission has joined others in the global community to educate and establish a culture of security. For example, we played a leading role in developing and implementing the OECD Security Guidelines, assisted in developing and promoting a website dedicated to the global dissemination of information about the Guidelines,[30] and play an ongoing role in information privacy and security work undertaken by the OECD and the Asian Pacific Economic Cooperation ("APEC") forum.[31]

D. Encouraging the Development and Deployment of Information Security Technologies

The Commission also encourages the development and deployment of information security technologies that may help protect consumers from spam and "phishing" attacks. In its June 2004 Report to Congress concerning a possible National Do Not Email Registry, the Commission identified domain-level authentication as a promising technological development that would enable ISPs and other domain holders to better filter spam, and that would provide

law enforcement with a potent tool for locating and identifying spammers.[32] Domain-level authentication could also serve as a useful tool in preventing "phishing" spam and spam containing viruses from reaching consumers' inboxes. The Report concluded that the Commission could play an active role in spurring the market's development, testing, evaluation, and deployment of domain-level authentication systems. As a first step, the Report explained that the Commission, with other relevant government agencies, would hold an Email Authentication Summit in the Fall of 2004. The Commission and the Department of Commerce's National Institute of Standards and Technology will be hosting the Summit on November 9-10, 2004.

E. Assisting Identity Theft Victims

Through our efforts to promote information security and educate consumers, we hope to prevent identity theft before it occurs. When identity theft does occur, however, we also have an extensive program to help consumers who have been victimized. The program has three principal components: (1) collecting complaints and providing victim assistance through a telephone hotline and a dedicated website; (2) maintaining and promoting the Identity Theft Data Clearinghouse, a centralized database of victim complaints that serves as an investigative tool for law enforcement; and (3) outreach and education to consumers, law enforcement, and private industry.

Victims may call the FTC through a toll-free hotline, 1-877-ID THEFT (438-4338), to receive telephone counseling from specially trained personnel. The phone counselors provide general information about identity theft and help guide victims through the steps needed to resolve the problems that result from the misuse of their identities.

The FTC also maintains the federal government's identity theft website, www.consumer.gov/idtheft, which includes publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources. Consumers may file identity theft complaints on our secure online complaint form. These complaints are entered into the Identity Theft Data Clearinghouse and are used by law enforcement agencies to support their investigations.

The Commission also is currently working on a number of rulemakings implementing provisions of the FACT Act that provide new and important measures to facilitate identity theft victims' recovery. These include a national fraud alert system, which will eliminate the need for victims to contact each of the major credit reporting agencies separately,[33] and identity theft blocking, which will prevent fraudulent account information from being reported on consumer reports.[34] When fully implemented, these initiatives should help to reduce the incidence of identity theft, and help victims recover when the problem does occur. In addition, the Commission is consulting with the Treasury Department on its study, required by the FACT Act, of how the use of biometrics and similar authentication technologies to identify parties to a transaction might reduce the incidence of identity theft.[35]

V. CONCLUSION

Through a variety of education and enforcement initiatives, the FTC is working to ensure that all companies entrusted with personal information take reasonable steps to secure that information and minimize the risk that it may be misused. The agency has been and will continue to be vigilant in promoting a culture of security. We are educating consumers and businesses about the risks to personal information and the role they must play in enhancing

security. We also will continue to assist victims of identity theft. In addition, the Commission will continue to take action against companies that violate information security laws.

ENDNOTES

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

2. The FTC's role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act"). Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028). The Act did not confer on the FTC any additional law enforcement authority.

3. Social Security numbers in particular play a pivotal role in identity theft. Identity thieves use the Social Security number as a key to access the financial benefits available to their victims.

4. For example, our 2003 Identity Theft Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf, showed that over 27 million individuals have been victims of identity theft, which may have occurred either offline or online, in the five years preceding the survey, including almost 10 million individuals in the year preceding the survey. The survey also showed that the average loss to businesses was $4800 per victim. Although in most cases, identity theft victims are not held liable for the fraudulent charges, they nonetheless suffer an average financial loss of $500, which reflects out-of-pocket expenses related to the efforts to dispute the frauds and repair their credit standing.

5. The Advisory Committee was comprised of forty e-commerce experts, industry representatives, security specialists, and consumer and privacy advocates. Information about the Advisory Committee, including its charter, membership, meeting transcripts, and working papers, is available at http://www.ftc.gov/acoas/index.htm. The Advisory Committee submitted its Final Report to the Commission in May 2000. The Report recommended that companies undertake a security approach that is appropriate to the circumstances, and advised that a good security program includes: conducting a risk assessment; establishing and implementing a security system; managing policies and procedures based on the risk assessment; conducting periodic training for employees; conducting audits; conducting internal reviews; and conducting periodic reassessment of risk. *See Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security* (May 15, 2000), available at http://www.ftc.gov/acoas/papers/finalreport.htm.

6. 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Pursuant to Section 501(b) of the Gramm-Leach-Bliley Act, the federal banking agencies have issued similar security guidelines that apply to the financial institutions they regulate. *See Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS).

7. In 2002, the OECD issued a set of nine voluntary principles for establishing a culture of security. The OECD principles are contained in a document entitled "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security." The principles address awareness, accountability, and action. They also recognize that security architecture and procedures should be appropriate for the kind of information collected and maintained and that good security is an ongoing process of assessing and addressing risks and vulnerabilities. *See* http://www.oecd.org/dataoecd/16/22/15582260.pdf.

8. The FTC has developed a kit, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, that provides advice on which law enforcement agency to contact, business contact information for the three major credit reporting agencies, suggestions for establishing an internal communication protocol, and information about contacting the FTC for assistance. The kit also provides FTC guidance regarding whether and how to notify consumers that there has been a breach. The information compromise kit is posted on our identity theft website, http://www.consumer.gov/idtheft and is also available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm.

9. Under certain state laws, companies may be required to notify consumers in the event of a breach. For example, the State of California requires consumer notification in the event of certain security breaches. The law, which went into effect July 1, 2003, requires a business or a State agency that maintains unencrypted computerized data that includes personal information to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver's license or state ID card number, or financial account numbers. *See* Cal. Civ. Code §§ 1798.29; 1798.82-1798.84.

10. The FTC's kit also includes a model letter for notifying individuals when that might be appropriate, such as when their names and Social Security numbers have been taken. Organizations are encouraged to print and include copies of *Identity Theft: When Bad Things Happen to Your Good Name* with the letter to individuals.

11. Prompt notification by businesses also alerts these individuals to review their credit reports and to watch for the signs of identity theft. In the event that individuals become victims, they can take action quickly to clear their records before any long-term damage is done.

12. The Federal Trade Commission maintains a database of identity theft complaints, and makes available and refers these complaints to criminal law enforcement agencies for investigation. Most identity theft cases are addressed best through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft, such as "pretexting" (tricking consumers or banks into revealing financial information) (*see, e.g.*, *FTC v. Corporate Marketing Solutions, Inc.*, Civ. No. 02-1256-PHX (RCB) (D. Ariz. Feb. 3, 2003) (final order)) or "phishing" (using spam email that looks like

it comes from a legitimate website to deceive consumers into providing account or other sensitive information) (*see, e.g., FTC v. M.M.*, Civ. No. 04-2086 (E.D.N.Y. May 18, 2004) (final order)). In addition, the FTC brought six complaints against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. *Press Release, Federal Trade Commission, FTC Targets Sellers Who Deceptively Marketed International Driver's Permits over the Internet and via Spam* (Jan. 16, 2003) (at http://www.ftc.gov/opa/2003/01/idpfinal.htm).

13. Pub. L. No. 108-159 (2003).

14. The FTC staff released a short staff summary of the findings from the workshop, which is available at http://www.ftc.gov/bcp/workshops/technology/index.html.

15. *See* Staff Workshop Report: Technologies for Protecting Personal Information, at 2-3.

16. *Id.* at 4-5.

17. In particular, the National Academies of Science and the Center for Democracy and Technology discussed the strengths and weaknesses of certain identity systems, and the distinctions between identification, authentication, and authorization.

18. *See* http://www.ftc.gov/infosecurity.

19. *Security Check: Reducing Risks to Your Computer Systems*, available at http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm.

20. *Detect, Protect, Disinfect: Consumers On Line Face Wide Choices in Security Products*, available at http://www.ftc.gov/bcp/conline/pubs/alerts/idsalrt.htm.

21. These include the consumer education website, www.staysafeonline.info.

22. 15 U.S.C. § 45.

23. 15 U.S.C. § 45(a)(1).

24. The Commission and the courts have defined a deceptive practice as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances. Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the Commission's Deception Policy Statement). The Commission also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. 15 U.S.C. § 45(n). The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with "phishing." *See FTC v. Hill*, Civ. No. H 03-5537 (filed S.D. Tex. Dec. 3, 2003),

http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm; *FTC v. C.J.*, Civ. No. 03-CV-5275-GHK (RZX) (filed C.D. Cal. July 24, 2003), http://www.ftc.gov/os/2003/07/phishingcomp.pdf.

25. *See MTS, Inc. d/b/a Tower Records/Books/Video*, FTC Dkt. No. C-4110 (June 2, 2004); *Guess?, Inc.*, FTC Dkt. No. C-4091 (August 5, 2003); *Microsoft Corp.*, FTC Dkt. No. C-4069 (Dec. 24, 2002); *Eli Lilly, Inc.*, FTC Dkt. No. C-4047 (May 10, 2002). The complaints and decisions and orders in these cases are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

26. The Rule requires covered financial institutions within the Commission's jurisdiction to develop a written information security plan to protect customer information that is reasonable in light of a company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each financial institution must include certain basic elements, including: (1) designating one or more employees to coordinate the safeguards; (2) identifying and assessing the risks to customer information in each relevant area of the company's operation, and evaluating the effectiveness of the current safeguards for controlling these risks; (3) designing and implementing a safeguards program, and regularly monitoring and testing it; (4) hiring appropriate service providers and contracting with them to implement safeguards; and (5) evaluating and adjusting the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

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

28. The FACT Act amends the Fair Credit Reporting Act in a number of ways, including the addition of a number of provisions intended to combat consumer fraud and related crimes, including identity theft.

29. *See* Disposal of Consumer Report Information and Records, 69 Fed. Reg. 21,388 (2004) (to be codified at 16 C.F.R. Part 682), available at http://www.regulations.gov/fredpdfs/04-08904.pdf. To help prevent identity theft, the FACT Act also directs the Commission to issue a "red flags" rule. *See* Pub. L. No. 108-396, § 157 (2003). The rule will help creditors analyze identity theft patterns and practices so that they can take appropriate action to prevent this crime.

30. *See* http://www.oecd.org/sti/cultureofsecurity.

31. The APEC Electronic Commerce Steering Group ("ECSG") promotes awareness and responsibility for cybersecurity among small and medium-sized businesses that interact with consumers. Commission staff participated in APEC workshop and business education efforts this past year and will remain actively engaged in this work for the foreseeable future.

32. The Commission's National Do Not Email Registry Report is available at: http://www.ftc.gov/reports/dneregistry/report.pdf.

33. Pub. L. No. 108-396, § 112 (2003).

34. Pub. L. No. 108-396, § 152 (2003).

35. Pub. L. No. 108-396, § 157 (2003).

Mr. PUTNAM. Our next witness is Steven Martinez. Mr. Martinez began work for the FBI in 1987. He has held a variety of supervisory and investigative positions within the FBI throughout the United States. In February 2003, Mr. Martinez was assigned as the FBI's first on-scene commander at CENTCOM, or Central Command, in Doha, Qatar, and in Baghdad, Iraq, in the staging of Operation Iraqi Freedom. While there he was in charge of all deployed FBI personnel and managed the FBI's counterterrorism and counterintelligence efforts spanning the initial combat phase of the war.

Mr. Martinez was appointed to his current position as Deputy Director of the Cyber Division in August 2004.

Welcome to the committee, Mr. Martinez. You are recognized. Welcome home.

Mr. MARTINEZ. Thank you, Mr. Chairman.

Again, good afternoon, Mr. Chairman and members of the subcommittee. I want to thank you for the opportunity to testify today regarding the FBI's efforts to combat identity theft as well as overlapping cybercrime problems.

Some studies show that last year alone more than 10 million victims were victimized by identity theft, with estimated losses exceeding $50 billion. These efforts demonstrate the significant impact identity theft has on U.S. citizens and businesses.

Identity theft is a growing problem and can manifest itself in many ways, to include large-scale intrusions into third-party credit card processors, theft from the mails of printed checks and preapproved credit cards, credit card skimming, phishing schemes and other cyber-related crimes.

More than 2 years ago, the FBI prioritized and restructured its approach to cybercrime with the establishment of the Cyber Division. Under the Cyber Division, the Internet Crime Complaint Center, or IC3, has focused on combating identity theft through the development of joint investigative initiatives with both our law enforcement partners and key e-commerce stakeholders. The IC3 receives on average more than 17,000 consumer complaints every month. Of the more than 400,000 complaints referred to the IC3 since its opening in May 2000, more than 100,000 can be characterized as identity theft.

The FBI is working to combat identity theft on many fronts, to include targeting criminal spammers. Spam is often the front end of a number of cybercrime scenarios used to invite unsuspecting customers to provide personal, financial or credit card information. Multiple agency operations, coordinated by the FBI to include Operation Web Snare, SLAM-Spam, Cyber Sweep and E-Con, has successfully launched hundreds of identity theft investigations. These investigations, involving thousands of U.S. victims and millions in dollars of losses, have resulted in the successful identification and arrest of hundreds of subjects. These operations further serve to alert both customers and industry about new or evolving schemes to which they may fall victim to identity theft.

Integral to each of such initiatives are public service advisories, which are developed in coordination with the FBI, our law enforcement partners and the FTC. These advisories are posted on law enforcement and industry Websites in order to warn the public about Internet identity theft scams.

The FBI has also seen an increase in identity theft matters with a foreign nexus to include a number of subjects from Eastern Europe and Africa. Many of these subjects solicit their victims through Internet job postings, e-mail, chat rooms, requesting detailed personal information under the guise of offering legitimate employment opportunities.

In response, the FBI has developed a close working partnership with many international law enforcement agencies, frequently providing agents and resources abroad in order to directly go after perpetrators.

Finally, computer intrusions can also significantly contribute to the problem of identity theft. One such instance involved the hacking of an e-commerce company system resulting in the network compromised and extortion of over 100 U.S. banks; 30 million credit card accounts, including subscriber information, were stolen as a result of the compromise.

The FBI takes a proactive role in working to investigate these types of cases to include maintaining close private industry contacts through programs such as InfraGard, a public-private alliance of more than 13,000 members.

In closing, the problem of identity theft is a significant matter, impacting the life and livelihood of U.S. citizens. The FBI appreciates the opportunity to share with you our efforts and successes in addressing this problem. The FBI will continue to combat identity theft so that America's citizens and the economy can be protected. Thank you.

Mr. PUTNAM. Thank you very much, Mr. Martinez.

[The prepared statement of Mr. Martinez follows:]

Testimony of Deputy Assistant Director
of the Federal Bureau of Investigation
Steven M. Martinez
before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
September 22, 2004

Introductory Statement:

Good afternoon Mr. Chairman and members of the subcommittee. I want to thank you for the opportunity to testify before you today about the FBI's efforts to combat Identity Theft, as well as other overlapping cyber crime problems.

Some studies show that more than 10 million Americans were victimized by Identity Theft in the space of one year, with estimated losses exceeding 50 billion dollars. These estimates demonstrate the significant impact on U.S citizens and businesses. Accordingly, targeting Identity Theft, and related cyber crime activity, will remain a priority of the FBI.

As you may be aware, the FBI prioritized and restructured its approach to cyber crime, in its many forms, a little more than two years ago, with the establishment of the Cyber Division. Several important premises were acknowledged as the foundation for this re-tooling. These included the need for increased law enforcement collaboration and the recognition that Subject Matter Experts (SMEs) from industry are often better positioned to identify and develop information regarding cyber crime incidents before law enforcement. Also, cyber crime does not often lend itself to a constricted list of terms or definitions. In fact, one incident of cyber crime can often be characterized using different labels such as

Identity Theft, Phishing, Credit Card Fraud, Account Hijacking, Computer Intrusion, Hacking, and even theft of Intellectual Property. Even if a more narrow definition of Identity Theft was adopted by law enforcement, it is important to note that the general public bases its definition on that which is portrayed through the TV, print and web-based media, which to date has been very broad.

In recognition of this fact, and the overriding need to gather the most complete and accurate intelligence as quickly as possible, in December of 2003 the FBI's Internet Fraud Complaint Center was renamed the Internet Crime Complaint Center (IC3). Also during this time period, the FBI focused its efforts on developing joint investigative initiatives with our partners in law enforcement, as well as key Internet E-commerce stake holders. These initiatives targeted escalating cyber crimes, both domestically and internationally, and invariably included numerous incidents which could be characterized as Identity Theft.

It should be noted that Identity Theft in its many forms is a growing problem and is manifested in many ways, including large scale intrusions into third party credit card processors; theft from the mails of printed checks, pre-approved credit card offers and mortgage documents; credit card skimming; Phishing schemes; telephone and bank frauds and other crimes.

Prior Testimony of Assistant Director Jana Monroe regarding SPAM:

When FBI Cyber Division Assistant Director Jana Monroe testified before the Senate Committee on Commerce, Science, and Transportation in May of this year, she reported on the FBI's SLAM-Spam initiative, which was developed jointly with law enforcement, industry, and the Federal Trade Commission, and which continues today. This initiative targets significant criminal spammers, as well as companies and individuals

that use spammers and their techniques to market their products. The SLAM-Spam initiative also investigates the techniques and tools used by spammers to expand their targeted audience, to circumvent filters and other countermeasures implemented by consumers and industry, and to defraud customers with misrepresented or non-existent products.

As you may be aware, SPAM is often the "Front End" of a number of cyber crime scenarios. SPAM, which in some cases has been criminalized with the passage of the Can Spam Act of 2003, is used to invite unsuspecting consumers to provide personal, financial, or credit card information, or to visit another site where malicious code, spyware, or another form of a so-called "Trojan horse" (back door) can be installed on their computer for later use. As a result of this initiative, more than 20 Cyber Task Forces are actively pursuing more than 30 criminal and, in some cases, joint civil proceedings against subjects identified to date.

Operation WEB-SNARE:

Several cases against such spammers were recently included in Operation WEB-SNARE, which, on August 26, 2004, was characterized by the Attorney General as the most successful cyber crime initiative to date. In WEB-SNARE, more than 150 investigations were successfully advanced, in which more than 150,000 victims lost more than $215 million. This initiative included 150 subjects who were charged, and the execution of 170 search and/or seizure warrants. Many of the investigations included in WEB-SNARE could potentially be characterized as Identity Theft, or related to Identity Theft.

Operations E-Con & Cyber Sweep:

Prior to WEB-SNARE, the IC3 coordinated the development and execution of Operations E-Con and Cyber Sweep with our law enforcement and industry partners. In those initiatives, more than 200 investigations were coordinated among the various law enforcement agencies, resulting in arrests and/or charges of more than 250 individuals for engaging in a variety of cyber crimes including Identity Theft.

In addition to demonstrating law enforcement's continued emphasis on cyber crime matters, such initiatives serve as a vehicle to alert consumers and industry about new or evolving schemes to which they may fall victim. Integral to each such initiative are Public Service Advisories or Consumer Be-Ware tips, which are developed in coordination with our federal partners in law enforcement and the FTC, and are included in materials distributed or posted on both law enforcement and industry web-sites. Some examples of these advisories and alerts which have been included in these initiatives have been warnings/alerts regarding Internet employment scams, the Reshipper Fraud, and information regarding Phishing attacks.

Phishing Initiative:

Phishing schemes have a consistent nexus to Identity Theft. Phishing is the creation and use of fraudulent but legitimate looking e-mails and web sites to obtain Internet users' identities and financial account information for criminal purposes. Internet users, who believe they have received an authentic solicitation for information from an entity with which the user has a trusted relationship, are duped into providing their sensitive personal information to criminals who have "spoofed" the e-mails and web sites of the trusted companies and/or government agencies with whom the victims believe they are interacting.

The most frequent targets of interest for criminals conducting such attacks are web sites belonging to the financial services sector, ISPs, and on-line auction venues.

Criminals who engage in Phishing often employ spamming (mass e-mail) techniques to send the Phishing e-mails to thousands or even millions of potential victims nearly simultaneously. Thus, Phishing can be a lucrative criminal enterprise even if only a small percentage of the recipients are deceived into disclosing their personal financial and/or other sensitive information.

Using the Public/Private Alliance model developed for the SLAM-Spam project which proved effective in bringing law enforcement and SMEs to a common venue to address cyber crime, a spin-off initiative is currently being developed to target Phishing. This project is being jointly developed with approximately 40 SMEs from 25 separate industry organizations that have agreed to join law enforcement in this project. This project is being developed jointly between the FBI, U.S. Postal Inspection Service, United States Secret Service, and the FTC, and is expected to be officially launched over the next 30 days.

The Cyber Division is also working closely with the FBI's Criminal Investigative Division, our law enforcement partners, and private industry, on an Identity Theft Working Group, which is actively engaged in intelligence sharing and coordination of public/private investigative efforts to address this crime problem.

International Aspects:

The FBI, through the IC3, has observed a continuing increase in both volume and potential impact of cyber crime with significant international elements. Identifying such trends, as well as formulating an aggressive and proactive counter-attack strategy, remains

a fundamental objective of the FBI's Cyber Division.

In a growing number of cases, Eastern European subjects solicit victims though job postings, email solicitations, and chat-rooms to provide detailed personal information. Once that information is obtained, they use their identities to post auctions on well-known auction sites. Funds obtained through the auction are transferred through several shell accounts, both in the U.S and abroad, and the items sold are never delivered.

In a similar "work at home" variation of this scheme, victims are also required to provide sensitive personal information as part of the application process. Such information is often used to register fraudulent auction sites or to obtain bogus credit cards and may be considered Identity Theft. Once "hired," victims receive packages containing computers and other high-price electronic equipment (usually purchased from on-line retailers with stolen/fraudulent credit cards) with instructions to repackage the items and ship them to locations in Eastern Europe. The victim is provided a cashier's check as payment, typically for several thousand dollars over the amount of the victims' agreed upon salary. Victims are instructed to deposit the check, deduct their salary, and wire the balance to the parent company located in Eastern Europe. Of course, the cashier's checks are later determined to be counterfeit.

West African Re-shippers:

These rapidly expanding schemes often originate in West Africa. A typical scenario includes subject purchases of merchandise from on-line vendors with stolen/fraudulent credit cards, listing a "domestic ship-to location" to allay concerns regarding suspicious international shipping orders, which are scrutinized and often denied by many E-Commerce merchants.

An expansive network of re-shippers continues to be recruited and utilized by subjects of these schemes. Recruitment is done via Internet Relay Chat (IRC) chat rooms, web based job postings, and even telephone solicitations. In return for the use of their residence or business address, the recruited re-shippers are often allowed to keep certain merchandise as payment, or are paid with counterfeit cashiers checks. New information indicates this scam may also have a European nexus. The potential economic impact is estimated to exceed $10 billion.

In coordination with law enforcement and industry partners, the FBI through the IC3, has identified 19,000 fraudulent transactions this year alone, involving more than $11 million in losses. Through recently enhanced cooperation with International Law Enforcement in Ghana and Nigeria, 31 individuals have been arrested and 34 seizures conducted in those countries involving approximately $1 million in merchandise.

IC3 Complaints Involving Identity Theft:

The IC3 is a joint project between the FBI and the National White Collar Crime Center (NW3C). The IC3 receives, on average, more than 17,000 complaints every month from consumers alone (18,999 in July 2004) and additionally receives a growing volume of referrals from key E-commerce stakeholders. Currently, over 25 percent of all complaints to the IC3 involve some use of spam electronic mail.

Of the more than 400,000 complaints referred to the IC3 since its opening in May of 2000, more than 100,000 were either characterized as Identity Theft, or involved conduct that could be characterized as Identity Theft.

Currently the FBI has more than 2,700 pending investigations of cyber crime matters, not including cases involving online sexual exploitation of children (i.e., our

"Innocent Images" initiative). Of the more than 1,800 cyber crime investigations opened in FY 2004, 346 individuals have been convicted with more than 942 million dollars in restitutions and recoveries.

Computer Intrusions/Hackers:

Computer intrusions, or hackers, can significantly contribute to the impact and scope of identity theft. In one FBI investigation initiated in 1999, the computer network of a now defunct software E-commerce company was compromised, and credit card information for approximately eight million accounts was obtained by the hackers. The compromised E-commerce company was contacted via email by the hackers who demanded money to keep them from publicly posting the obtained information on the Internet.

The FBI became aware of this crime when numerous field offices received complaints from citizens who were all incorrectly charged for similar small amounts on their credit card statements. Through investigative efforts, these complaints were all linked to the hacking of the E-commerce company's system. This case has expanded into a major FBI initiative in which field offices across the country have opened approximately 50 spin-off investigations in the network compromise and extortion of over 100 United States banks and E-commerce providers by Eastern European hacking groups.

Thirty million credit card accounts, including subscriber information, have been stolen as a result of these systems being compromised. The subscribers' information obtained through these computer intrusions contained enough information to create false identifications, open bank accounts, apply for loans, and otherwise pose as the original cardholder. Based on a consensus figure of $500 per account, this represents a potential

loss of $15 billion.

This investigation required the FBI to build upon its international relationships and establish strong ties with foreign law enforcement agencies. Thus far, three of the main subjects of this group have been prosecuted in the U.S., and two others have been prosecuted abroad. Currently, there are five outstanding complaints against the remaining international subjects.

Participation of InfraGard Membership:

InfraGard is an FBI program that began in the Cleveland Field Office in 1996 as a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. Today InfraGard has expanded to all FBI Field Offices with approximately 13,000 members ranging from representatives of Fortune 500 companies to the owners of small ISPs.

At its most basic level, InfraGard is a cooperative undertaking dedicated to sharing information and intelligence derived from various FBI cyber related investigations. InfraGard provides a forum for dialogue and relationship building between policy makers, private companies, and the law enforcement community on a number of issues. Its goal is to enable two way information flow so that the owners and operators of systems and networks can better protect themselves, and, as a result, the United States Government can better discharge its law enforcement and national security responsibilities.

The InfraGard membership regularly provides intelligence and referrals that assist law enforcement's efforts to identify and counter the most significant criminal and national security threats to our country's networks.

Available Statutes:

In addition to the CAN SPAM ACT of 2003, such schemes might be prosecuted through Title 18, USC 1028 (Fraud and related activity in connection with Identity documents), Title 18, USC 1029 (Fraud and related activity in connection with Access Devices), Title 18, USC 1030 (Fraud and related activity in connection with computers), Title 18 USC 2319 (Criminal Infringement of a copyright), Title 18 USC 1343 (Fraud by Wire), Title 18 USC 1341 (Mail Fraud), and Title18 USC 1028A (Identity theft penalty enhancements).

Conclusion:

Once again, I appreciate the opportunity to come before you today and share the work that the Cyber Division has undertaken to address the problem of Identity Theft. The FBI's efforts in this arena will continue, and we will continue to keep Congress informed of our progress in protecting the America's citizens and economy.

Mr. PUTNAM. Our next witness is Larry Johnson. Mr. Johnson has been a part of the Secret Service for 22 years and has held supervisory positions in both its Protective and Investigative Divisions. He currently holds the title of Special Agent in Charge of the Criminal Investigative Division and is responsible for the oversight of the Secret Service's criminal investigations, both domestic and abroad. The Criminal Investigative Division also manages the Secret Service's electronic crime programs and initiatives, including the specialized training of agents in computer forensics and the developments and implementation of the Secret Service's electronic crime task forces.

Welcome to the subcommittee, sir, you are recognized for 5 minutes.

Mr. JOHNSON. Chairman Putnam, Mr. Clay, members of the subcommittee, thanks for inviting me today.

In addition to providing the highest level of physical protection to our Nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As an original guardian of our Nation's financial payment system, the Secret Service has a long history of protecting American customers and industry from financial fraud. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism have caused the investigative mission of the Secret Service to evolve dramatically. The explosive growth of these crimes has resulted in the elevation of the Secret Service to an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

In today's markets, customers routinely provide personal and financial identifiers to companies engaged in business on the Internet. Information trading and the wealth of personal information available creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders.

Internet crime has increased significantly in the last several years. Since the early 1990's, organized computer underground networks have developed an extraordinary record of malicious software development. Starting in the late 1990's and increasing over the last few years, this criminal element has used such malicious software to penetrate financial and government institutions, extract data and illicit traffic in stolen and financial identity information.

Criminal networks engage in electronic financial fraud, participate in a wide range of activities in order to make their scheme successful. They first obtain and store financial data for future exploitation. Gaining access to this data involves various techniques, technical methods, including hacking, virus-writing, phishing and skimming.

The criminal underground active in credit card fraud and identity theft crimes has rapidly adapted its operations to an on-line world, where it has found convenient solutions to the age-old problems in the forms of anonymous communication networks, as well as global, unregulated movement of illegally obtained funds.

This has created new challenges for Federal and local law enforcement agencies. By working closely with international police

agencies, other Federal, State and local law enforcement, the Secret Service is able to provide a comprehensive network of ongoing investigative operations, intelligence sharing, resource sharing and technical expertise that has bridged judicial boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects in criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service. Members of these task forces, who include representatives from local and State law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes and identity theft.

The value of this crime-fighting and crime-prevention model has been recognized by Congress, which has authorized the Secret Service, pursuant to the U.S. Patriot Act of 2001, to expand our electronic crimes task forces to cities and regions across the country. Two new electronic crime task forces will be established this month, bringing the total number of ECTFs to 15.

The Secret Service Electronic Crimes Task Force Program bridges the gap between conventional cybercrime investigations and the larger picture of critical infrastructure protection. Secret Service efforts to combat cyber-based assaults that target information and communications systems supporting the financial sector are a part of the larger and more comprehensive critical infrastructure protection.

A key element in our strategy of sharing information and operating with other Federal agencies, to include IC3, the department of Treasury, Department of State and the FBI, are the 17 permanent U.S. Secret Service field offices that support both our protective and investigative missions. The Secret Service provides training for counterfeit investigations, financial crimes and computer intrusions to our international law enforcement partners.

In a joint effort with the Department of Justice, the U.S. Postal Inspection Service, the FTC and the International Association of Police Chiefs, the Secret Service is hosting identity crime training seminars for local enforcement officers across the country. These training seminars are focused on providing local and State law enforcement officers with tools and resources that they can immediately put to use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

The Secret Service will continue its aggressive domestic and international pursuit of cybercriminals who are involved in the hacking of our Nation's computer systems, the intrusions of our networks and the theft of identities of U.S. citizens through mainly prevention and disruption. The Secret Service, with the assistance of the Department of Homeland Security, is committed to the deterrence and apprehension of all potential cybercriminal suspects who threaten citizens of the United States and its critical infrastructure.

Mr. Chairman, that concludes my prepared statement.

Mr. PUTNAM. Thank you very much, Mr. Johnson.

[The prepared statement of Mr. Johnson follows:]

STATEMENT OF LARRY D. JOHNSON

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Before the Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census

U.S. House of Representatives

September 22, 2004

Good afternoon, Mr. Chairman. I would like to thank you, as well as the distinguished Ranking Member, Mr. Clay, and the other members of the subcommittee for providing an opportunity to discuss the subject of information security, and the role of the Secret Service in safeguarding our financial and critical infrastructures.

In addition to providing the highest level of physical protection to our nation's leaders, the Secret Service exercises broad investigative jurisdiction over a wide variety of financial crimes. As the original guardian of our Nation's financial payment systems, the Secret Service has a long history of protecting American consumers and industry from financial fraud. For two decades, the Secret Service has been the primary federal law enforcement agency responsible for the investigation of access device fraud, including credit and debit card fraud. In addition, we have concurrent authority with other law enforcement agencies in identity crime cases. In recent years, the combination of the information revolution, the effects of globalization and the rise of international terrorism has caused the investigative mission of the Secret Service to evolve dramatically. The explosive growth of high tech and international crimes has led the Secret Service to become an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes. Our efforts to detect, investigate and prevent financial crimes are aggressive, innovative and comprehensive.

After 138 years in the Treasury Department, the Secret Service was transferred last year to the Department of Homeland Security with all of its personnel, resources and investigative jurisdictions intact. Today, those responsibilities require us to be involved in the investigation of traditional financial crimes as well as identity crimes and a wide range of electronic and high-tech crimes.

The burgeoning use of the Internet and advanced technology, coupled with increased investment and expansion, has intensified competition within the financial sector. While these advances have produced a number of benefits to consumers, we must also recognize that with lower costs of information-processing, legitimate companies have found it profitable to specialize in data mining, data warehousing and information brokering. Information collection has become a common byproduct of newly-emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by businesses seeking to find the best customers for their products. This has led to a new measure of growth within the direct marketing industry that promotes the buying and selling of personal information.

In today's markets, consumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card or loan applications, or to merchants they patronize is a valuable commodity in this new age of information trading. Consumers may be even less aware of the illegitimate uses to which this information can be put. This wealth of available personal information creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime, even while not eliminating its occurrence altogether.

Identity crime is the theft or misuse of an individual's personal or financial identifiers in order to gain something of value or to facilitate other criminal activity. Types of identity crime include identity theft, credit card fraud, bank fraud, check fraud, false identification fraud and passport/visa fraud. It is equally important to note that identity crimes are used to facilitate and fund other serious crimes such as narcotics and weapons trafficking, organized crime, mail theft and fraud, money laundering, immigration fraud and terrorism. Identity crimes provide the anonymity for criminals to operate undetected and untraceable financing to fund their criminal endeavors.

According to statistics compiled by the Federal Trade Commission for 2003, 42% of the 516,740 victim fraud complaints reported involved at least one type of identity crime. The complaints were broken down as follows *(note that some complaints involved more than one of the listed activities)*:

- **33%** of complaints involved credit card fraud – i.e. someone either opened up a credit card account in the victim's name or "took over" his or her existing credit card account;

- **21%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;

- **17%** of complaints involved bank accounts opened in the victim's name, and/or fraudulent checks negotiated in the victim's name;

- **11%** of complaints involved employment-related fraud;
- **8%** of complaints involved government documents/benefits fraud;
- **6%** of complaints involved consumer loans or mortgages that were obtained in the victim's name; and
- **19%** of complaints involved some type of miscellaneous fraud, such as medical, bankruptcy and securities fraud.

Although financial crimes are often referred to as "white collar", this characterization can be misleading. The perpetrators of such crimes are increasingly diverse, and today include both domestic and international organized criminal groups, street gangs, convicted felons and terrorists.

These criminals seek the personal identifiers generally required to obtain goods and services on credit, such as social security numbers, names, and dates of birth. Identity crimes also involve the theft or misuse of an individual's financial identifiers such as credit card numbers, bank account numbers and personal identification numbers.

The methods of identity criminals vary. "Low tech" identity criminals obtain personal and financial identifiers by going through commercial and residential trash, a practice known as "dumpster diving". The theft of wallets, purses and mail is also a widespread practice employed by both individuals and organized groups.

With the proliferation of computers and increased use of the Internet, "high tech" identity criminals began to obtain information from company databases and web sites. In some cases, the information obtained is in the public domain; in others it is proprietary and is obtained by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. Individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through his or her employment at a workplace such as a utility billing center, financial institution, medical office or government agency. The collusive employee will access the proprietary data base, copy or download the information, and remove it from the workplace either electronically or simply by walking it out.

Once the criminal has obtained the proprietary information, it can be exploited by creating false "breeder documents" such as a birth certificate or social security card. These documents are then used to obtain genuine, albeit false, identification, such as a driver's license or passport. Now the criminal is ready to use the illegally-obtained personal identification to apply for credit cards or consumer loans or to establish bank accounts. This, in turn, leads to the laundering of stolen or counterfeit checks or to a check-kiting scheme. Our own investigations have frequently involved the targeting of

organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal identifiers to further their other criminal activity.

Recognizing that the United States Code provided an insufficient deterrent to the commission of identity crimes, Congress recently enacted the Identity Theft Penalty Enhancement Act. This act mandates an additional two-year sentence (or five years, in the case of some offenses) for anyone possessing or using, without lawful authority, a means of identification of another person during and in relation to the commission of numerous other Federal felonies. It is particularly important that this sentence cannot be served as probation or concurrently with any other term of imprisonment.

Agency Coordination

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created challenges for local law enforcement agencies that generally act as the first responders to such criminal activities. By working closely with our federal, state, and local law enforcement partners, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that fall within the investigative jurisdiction of the Secret Service.

Members of these task forces, who include representatives from local and state law enforcement, prosecutors' offices, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes. The value of this crime fighting and crime prevention model has been recognized by Congress, which has authorized the Secret Service to expand its electronic crime task forces to cities and regions across the country. Recently, four new Electronic Crimes Task Forces (ECTFs) were established in Dallas, Houston, Columbia (SC) and Cleveland, bringing the total number of such task forces to 13.

The Secret Service ECTF program bridges the gap between conventional cyber-crimes investigations and the larger picture of critical infrastructure protection. Secret Service efforts to combat cyber-based assaults that target information and communications systems supporting the financial sector are part of the larger and more comprehensive critical infrastructure protection and counterterrorism strategy.

As part of the Department of Homeland Security, the Secret Service continues to be involved in a collaborative effort targeted at analyzing the potential for financial, identity and electronic crimes to be used in conjunction with terrorist activities. The Secret Service prides itself on an investigative and preventive philosophy that fully involves our partners in the private sector and academia as well as our colleagues at all levels of law

enforcement in combating the myriad types of financial and electronic crimes. Central to our efforts in this arena are our liaison and information exchange relationships with the Bureau of Immigration and Customs Enforcement (ICE), the Department of the Treasury, the Department of State, and the FBI. As Secret Service investigations uncover activities of individuals or groups focusing on doing harm to the United States, appropriate contact is immediately made and information is passed to those agencies whose primary mission is counterterrorism.

As a key element in our strategy of sharing information and cooperating with other agencies involved in the effort to keep America safe, the Secret Service has assigned 58 Special Agents to the FBI's Joint Terrorism Task Forces (JTTFs) and additional personnel to Operation Cornerstone (led by ICE) and the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

The Secret Service currently has 17 permanent foreign offices that support both our protective and investigative missions. Agents in these offices work in cooperation with host country law enforcement officials and contribute to international information sharing and training as well as criminal investigations. The Secret Service also provides training for counterfeit investigations, financial crimes and computer intrusions to our international law enforcement partners.

The Secret Service is actively involved in a number of other government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of Justice (DOJ). This group, which comprises federal, state, and local law enforcement agencies, regulatory agencies, and professional organizations, meets regularly to discuss and coordinate investigative and prosecutorial strategies as well as consumer education programs.

In a joint effort with DOJ, the U.S. Postal Inspection Service, the Federal Trade Commission and the International Association of Chiefs of Police, we are hosting Identity Crime Training Seminars for law enforcement officers. In the last two years we have held seminars for officers in Chicago, Dallas, San Francisco, Las Vegas, Des Moines, Washington D.C., Phoenix, New York, Seattle, San Antonio, Providence, Orlando, Raleigh, Rochester and Denver. These training seminars are focused on providing local and state law enforcement officers with tools and resources that they can immediately put into use in their investigations of identity crime. Additionally, officers are provided resources that they can pass on to members of their community who are victims of identity crime.

Operation Direct Action (ODA) is a task force comprised of the Secret Service and a number of private sector partners. The primary focus of this task force is to target organized criminal groups that are committing large scale financial fraud, specifically credit card "bust out" schemes that may impact our nation's financial infrastructure. A "bust out" scheme is a type of fraud where a criminal obtains multiple credit card accounts and manipulates the lines of credit that are established with each card. The

criminal makes payments with convenience checks issued by another card or with Non-Sufficient Funds (NSF) checks drawn on any number of bank accounts. The criminal is taking advantage of the lag time between the credits to accounts and the issuing banks' determination that the checks were bad.

Preventative Efforts

Another important component of the Secret Service's preventative and investigative efforts is our focus on increasing awareness of issues related to financial crime investigations in general, and of identity crime specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity crime, now routinely involves the seizure and analysis of electronic evidence. In fact, so critical was the need for basic training in this regard that the Secret Service joined forces with the International Association of Chiefs of Police and the National Institute for Justice to create the "Best Practices Guide to Searching and Seizing Electronic Evidence" which is designed for the first responder, line officer and detective alike. This guide assists law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

We have also worked with these same partners in producing the interactive, computer-based training program known as "*Forward Edge*," which takes the next step in training officers to conduct electronic crime investigations. *Forward Edge* is a CD-ROM that incorporates virtual reality features as it presents three different investigative scenarios to the trainee. It also provides investigative options and technical support to develop the case. Copies of state computer crime laws for each of the fifty states as well as corresponding sample affidavits are also part of the training program and are immediately accessible for instant implementation.

Thus far, we have distributed over 300,000 "Best Practices Guides" to local and federal law enforcement officers and have distributed, free of charge, over 20,000 *Forward Edge* training CDs.

In addition, we have just completed the Identity Crime Video/CD-ROM which contains over 50 investigative and victim assistance resources that local and state law enforcement officers can use when combating identity crime. This CD-ROM also contains a short identity crime video that can be shown to police officers at their roll call meetings which discusses why identity crime is important, what other departments are doing to combat identity crime, and what tools and resources are available to officers. The Identity Crime CD-ROM is an interactive resource guide that was made in collaboration with the U.S. Postal Inspection Service, the Federal Trade Commission (FTC) and the International

Association of Chiefs of Police. To date, over 40,000 Identity Crime CD-ROMs have been distributed to law enforcement departments and agencies across the United States.

The Secret Service has also assigned a special agent to the FTC as a liaison to support all aspects of that agency's program to encourage the use of the Identity Theft Data Clearinghouse, the nation's central repository for identity theft complaints, as a law enforcement tool. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft.

It is important to recognize that public education efforts can only go so far in combating the growth of identity crime. Because social security numbers, in conjunction with other personal and financial identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

Mr. Chairman, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

Mr. PUTNAM. Our next witness is Patrick O'Carroll. Nice French name.

Mr. O'Carroll currently serves as the acting inspector general for the Office of the Inspector General of the Social Security Administration. In fiscal year 2003, the office of investigators has reported over $356 million in investigative accomplishments.

Prior to coming to the Social Security Administration, Mr. O'Carroll had 24 years of experience with the U.S. Secret Service. So we have two Secret Service representatives with us today. Throughout his career, Mr. O'Carroll has received numerous awards for his meritorious service.

Welcome to the subcommittee, sir. You are recognized for 5 minutes.

Mr. O'CARROLL. Good afternoon, Mr. Chairman and Mr. Clay. Thank you for the invitation today to be here for this important hearing. You have my statement for the record, so I will provide a few remarks.

Protecting information is vital to the Social Security Administration and its programs. Any breach in the confidentiality or integrity of their data would seriously jeopardize the agency's mission and erode the public's confidence in SSA programs. As part of the mission of the SSA Office of the Inspector General, we work closely with the agency to ensure that SSA has the proper controls in place to preserve the integrity of its data and business processes. Today I will focus on why it is important to prevent electronic data theft, what my office is doing to help SSA, some of SSA's data security efforts, and what more needs to be done.

The information technology revolution brings a heightened risk of disruption or sabotage of critical operations. We need to protect the public by preventing destruction and cyberattacks when possible, or ensuring that they are infrequent and manageable.

Another threat to our essential electronic data is identity theft, the fastest growing form of white-collar crime in America. Our investigations in this area reveal how widespread the misuse of SSNs and other sensitive data from public and private sector data bases has become.

The topic of identity theft is more than just dollars and numbers. Let me give you a specific example. We have recently received a letter from an individual who found that her and her husband's personal information was posted on a publicly available government Website complete with her Social Security number. In a letter to me, she indicated she had made multiple inquiries at the local, State and Federal level trying to have her personal information removed. The individual commented in her letter that the Government, both State and Federal, should do whatever is possible to ensure the integrity of every citizen's SSN. I couldn't agree more.

In addition to our efforts regarding SSN misuse, we also consider investigations of employee fraud a high priority. It only takes one corrupt employee to compromise the integrity of the Social Security system. In particular, illegally used SSNs puts the financial integrity of the SSA system at risk and inhibits the country's work for terrorism.

Let me discuss two of our successful investigations. In one, a 15-year SSA employee provided Social Security cards for a scheme in

which immigrants paid up to $75,000 for citizenship. The SSA employee resigned and was only sentenced to 2 months of incarceration.

In another, an SSA employee knowingly approved fraudulent applications for over 1,700 Social Security cards for approximately $1,000 each as part of a $4.3 million criminal enterprise. The SSA employee lost his job, was sentenced to 71 months in prison, and was ordered to forfeit $1 million.

SSA has made significant progress in strengthening SSN integrity and has implemented important suggestions which our office has made. SSA's efforts toward protection of electronic data include the SSA Enumeration Response Team comprised of agency executives, including OIG representatives, that has implemented numerous policies and procedures designed to better ensure that only individuals authorized to receive an SSN are available to do so.

The agency is also piloting an on-line Social Security number verification system, which will allow employers and third parties to verify employer names and SSNs via the Internet, using information and SSA records for wage-reporting purposes. This system will also indicate if the SSA record shows that an employee is deceased.

While SSA protects its data with numerous controls and safeguards, we are concerned about how other Federal agencies maintain security of SSNs. Given the potential risk, we believe Federal agencies would benefit by strengthening controls over the access, disclosure and use of SSNs by State and local governments and other external entities. Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently obtained drivers' licenses are keys to identity fraud in the United States. Our OIG works closely with SSA to help ensure the integrity of all of its data.

As technology has advanced, SSA has kept pace in developing appropriate safeguards against intrusion. SSA must continue to strike a balance between the need to be user-friendly and the demands for increased security. Together with Congress and SSA, we have made important strides in reducing vulnerabilities, and that effort continues.

Still, to strengthen our defenses even further, we believe that SSA should work with agencies across government to improve safeguards for data security. We also believe SSA and lawmakers should exam the feasibility of the following initiatives: limiting the SSN's public availability, prohibiting the sale of SSNs, and prohibiting their display on public records, and enacting strong enforcement mechanisms and stiffer penalties to discourage SSN issues.

I would be happy to answer any questions you may have.

[The prepared statement of Mr. O'Carroll follows:]

U.S. House of Representatives

Committee on Government Reform

Sub-committee on Technology, Information Policy,
Intergovernmental Relations and the Census

Statement for the Record

Theft of Electronic Data

Patrick P. O'Carroll, Jr.
Acting Inspector General of the Social Security Administration

September 22, 2004

Good morning, Mr. Chairman, Mr. Clay, and members of the Subcommittee. Let me first thank you for the invitation to be here today for this important hearing to discuss the theft of electronic data. The mission of the Social Security Administration (SSA) Office of the Inspector General (OIG) is to protect Social Security programs and operations from fraud, waste, and abuse. As the Federal agency that implements this country's retirement and social welfare programs, it is paramount that the information SSA collects and stores is secure and reliable. SSA maintains sensitive information from wage and earnings to medical information. Most notable is the Social Security number (SSN), which is used to link data to millions of individuals. Protecting Agency information is vital to SSA programs, and any breach of the confidentiality or integrity of its information would seriously jeopardize the Agency's mission and erode the public's confidence in SSA's programs.

In addition to protecting the theft of information held by SSA, we are also concerned about the integrity of the information SSA receives. While new technologies afford us greater flexibility in performing routine activities, they also present new opportunities for misuse. As government continues to embrace the electronic age and moves closer to paperless processing, we must be certain that appropriate safeguards are in place to verify the authenticity of every transaction. As part of our mission, we work cooperatively with the Agency to ensure that SSA has the proper controls in place to preserve the integrity of its data and business processes.

Today, I would like to discuss:

- Why it is important to prevent the theft of electronic data
- What OIG is doing to help SSA prevent electronic data theft
- SSA's electronic data security efforts
- What remains to be done

Why it is important to prevent the theft of electronic data

The information technology revolution has changed the way government and business operates. Today, the growth in computer interconnectivity brings a heightened risk of disruption or sabotage of critical operations, allowing unscrupulous individuals to read or copy sensitive data, and tamper with critical processes. Those who engage in these activities have more tools than ever before. We need to protect the public by preventing disruptions and ensuring that any disruptions are infrequent, manageable, of minimal duration, and cause the least damage possible.

The threat of electronic data theft and other cyber attacks is growing exponentially in severity, frequency, and financial cost. According to one estimate, cyber attacks last year alone cost the U.S. financial sector nearly $1 billion. These times of heightened national security demand coordinated efforts to protect computer systems from external and internal intrusion. We are pleased that this Subcommittee is rigorously assessing the Federal Government's progress to address weaknesses in the security of its computer systems—particularly the protection of information and data from the threat of cyber attacks, theft and other security breaches.

I am also concerned about the escalating occurrences of identity theft, a major result of electronic data theft and the fastest-growing form of white-collar crime in the United States. A year ago the Federal Trade Commission (FTC) reported that 27.3 million Americans were victims of identity theft between 1998 and 2003—including 9.9 million people in the study's final year. In 2003, losses to businesses and financial institutions totaled nearly $48 billion, and consumer victims reported $5 billion in out-of-pocket expenses. Clearly, this is a problem that must be brought under control.

What OIG is doing to help SSA prevent electronic data theft

Over the years, we have raised concerns in testimony and reports and have called for improved security for *all* databases—both public and private sector—that contain SSNs and other sensitive data, both as a homeland security issue and as an identity theft issue. Today, the SSN is a widely used identifier, which can be used to tie multiple records together about a single individual. While phone numbers, addresses, and even names can change, the SSN is constant throughout an individual's life. Because of this, many institutions, including hospitals and some banks and brokerages, use clients' SSNs as an identity confirmation. Other institutions, notably banks, use SSNs as secret passwords that only the owner should know.

While common use of the SSN as an identifier seems reasonable, it is an invitation for identity theft. For example, if someone knows the name and SSN of another individual, they could use this information to access accounts, transfer funds, or make other changes to an account, which has serious repercussions for the true account holder. When SSNs appear with their owners' names on driver's licenses, mailing labels, and university student ID cards, the owners of these SSNs become potential targets. In fact, we are currently reviewing the use of the SSN on student IDs in a nationwide audit that will examine such policies at approximately 100 schools. Perhaps the most important step we can take in preventing SSN misuse is to limit the SSNs easy availability on public documents, and even in electronic forums such as the Internet.

Our investigations in this area reveal how widespread the misuse of SSNs and other sensitive data from public and private sector databases has become. For example, we recently discovered an offer to sell up to 10,000 SSNs with matching names on the eBay web site. These SSNs were used by the University of North Carolina at Pembroke as identifiers for its staff, current students, and applicants. The suspect successfully stole these SSNs and was ultimately sentenced to 5 months' incarceration.

Our Philadelphia Field Division participated in an investigation that found that a former credit card company employee provided several co-conspirators personal information of legitimate account holders. The co-conspirators then used this information to open and transfer money from fraudulent accounts. The former employee was sentenced to 4 years probation and ordered to pay the bank restitution of over $132,800.

In another case, after a year-long identity theft investigation, our agents arrested a man who had more than 250 credit cards—along with identification documents and fraudulent Social Security cards—for aliases he used in an elaborate scheme he began while working as a credit manager at a local furniture store. When the company was sold and his job was terminated, he took several credit reports with him and used those SSNs to get credit cards, bank loans, homes, vehicles, computers and cash. He was sentenced to 25 months in prison, ordered to pay $383,000 in restitution to numerous credit card companies and banking institutions, and ordered to forfeit a home and a recreational vehicle.

The range of sources from which these SSNs and other critical personal information were stolen is alarming—legitimate web sites, universities, credit card companies, and a furniture store. It is not just SSA that has your number—numerous government agencies, companies and individual operators such as doctors and insurance agents have them as well. In fact, it is quite possible that your number has been given without your knowledge to numerous organizations, businesses and individuals. We cannot put the genie back in the bottle, but we must do more to make those who hold this critical information treat it with the same respect they would give to their own bank account numbers.

SSA employee fraud

Although the vast majority of SSA's over 60,000 employees are trustworthy, dedicated civil servants, it only takes one corrupt employees to compromise the integrity of the Social Security system and undermine the public's confidence in SSA's programs. The illicit demand for SSNs increases the profitability of providing genuine SSNs illegally to fraudulent applicants. Consequently, our investigations have found that a number of SSA employees have succumbed to this temptation. While employee fraud comprises very few allegations, we consider this an investigative priority.

I would like to give you a couple of examples of our successful investigations in this area. One scheme promised immigrants a Social Security card and U.S. citizenship for up to $75,000 per person. The woman who ran the operation staged naturalization ceremonies with a fake Federal judge, fraudulently obtaining genuine Social Security cards through a 15-year SSA employee. The ringleader was sentenced to 121 months in prison, and ordered to pay restitution of $349,065 to her victims. The SSA employee resigned and was sentenced to 2 months of incarceration. Two others received probation.

Another investigation revealed a $4.3 million criminal enterprise that provided Social Security cards and other credentials to undocumented aliens. Working with other agencies, we found that an SSA employee processed and knowingly approved fraudulent applications for over 1,700 Social Security cards for approximately $1,000 each. Illegally issued SSNs put the financial integrity of the Social Security system at risk, inhibit the country's efforts to thwart terrorism, permit the potential defrauding of other Federal and State programs, and compromise the safety of American citizens. The SSA employee involved in this scheme lost his job, was sentenced to 71 months in prison, and was ordered to forfeit $1 million and his residence in Lake Dallas, Texas. Three co-defendants were sentenced to as much as 63 months in prison, and another was given probation and home confinement.

We recently completed an audit of the Agency's policies and practices towards employees who have inappropriately accessed and used SSA's information systems and the sensitive information in the systems. We found that SSA has a process in place to review potential employee systems security violations and has taken steps to limit its exposure to employee misuse of its systems, and we have recommended additional improvements.

Other Federal agencies' use of the SSN

Within the confines of SSA, the SSN is protected with numerous controls. However, once SSNs are used for other purposes, SSA does not have control over, or the ability to protect, these numbers. The security of files containing SSNs maintained by agencies and organizations at every level of Government and the private sector is a serious concern to us.

Our 2003 audit report *"Federal Agencies' Controls Over the Access, Disclosure and Use of SSNs by External Entities,"* requested by the Chairman of the Subcommittee on Social Security, House Ways and Means Committee, examined the way Federal agencies disseminate and control the use of SSNs. After consultation with the President's Council on Integrity and Efficiency (PCIE), we agreed to serve as audit lead for 15 participating OIGs and to prepare the final report.

We found that despite safeguards to prevent improper access, disclosure and use of SSNs by external entities, Federal agencies remained at risk to such activity. Of the 15 agencies reviewed:

- Fourteen agencies lacked adequate controls over contractors' access to and use of SSNs (for example, eight agencies had not performed site inspections to ensure contractors had upheld their obligation to protect the confidentiality and security of SSNs).

- Nine agencies had inadequate controls over access to SSNs maintained in their computer systems (for example, one agency granted systems access to its employees before completing background security checks, while others were not monitoring user access to ensure users were still current employees or contractors).

- Two agencies did not have adequate controls over non-Government and/or non-contractor entities' access to and use of SSNs (for example, one OIG reported its agency had no standard contract language to include Privacy Act safeguards).

- One agency did not make legal and informed SSN disclosures (its OIG identified instances in which the agency did not inform research study participants that providing their SSNs was voluntary).

While Federal agencies' efforts cannot eliminate the potential that unscrupulous individuals may inappropriately acquire and misuse SSNs, we believe each Federal agency has a duty to safeguard the integrity of SSNs by reducing opportunities for external entities to improperly obtain and misuse them. Given the potential risk for individuals to engage in such activity, we believe Federal agencies would benefit by strengthening controls over the access, disclosure and use of SSNs by State and local governments and other external entities. Misused SSNs, stolen or misappropriated birth certificates, and false or fraudulently-obtained driver's licenses are the keys to identity fraud in the United States. With any one of these three documents, you can generally obtain the other two. We investigate thousands of SSN fraud and identity theft cases every year, and we often find criminals have not only stolen or forged SSN information, but stolen or forged driver's licenses as well. We maintain a strong working relationship with the American Association of Motor Vehicle Administrators (AAMVA) and have supported the development, deployment, and monitoring of commercial driver's license and motor carrier safety programs throughout the United States.

SSA's electronic data security efforts

SSA has made significant progress in strengthening SSN integrity, implementing important suggestions our office has made, and working with us to find solutions. In November 2001, the Commissioner of Social Security established an Enumeration Response Team (ERT) comprised of Agency executives, including OIG representatives, to identify steps the Agency could take to improve the enumeration process and to enhance the integrity of the SSN. Since that time, the Commissioner and the ERT have implemented numerous policies and procedures designed to better ensure that only individuals authorized to receive an SSN are able to do so. Earlier Agency initiatives included improving its Comprehensive Integrity Review Process to identify enumeration vulnerabilities.

The Agency has also has taken steps to improve the verification of employee data. For example, SSA assists employers with its Employee Verification Service (EVS) for registered employers. The Agency is also piloting an online Social Security Number Verification Service (SSNVS), which allows employers and third parties to verify employees' names and SSNs via the Internet, using information in SSA's records, for wage reporting purposes. SSNVS also indicates if SSA records show that the employee is deceased.

Employers have two online SSNVS options:

- Key in up to 10 names and SSNs at a time and the results are returned in seconds.
- Submit a file containing up to 250,000 names and SSNs per file and the results are returned the next business day.

SSNVS is beneficial because it:

- Helps employers use correct names and SSNs on wage reports.
- Reduces the number of submission errors.
- Offers an additional method of requesting verification services.
- Reduces the number of telephone calls required for employers to verify names and SSNs.

The importance of SSN integrity notwithstanding, I noted earlier that the Agency must secure *all* of its data. The President's Management Agenda (PMA) noted expanded e-Government as a presidential initiative across the Federal government. As we provide more online information and transactions, SSA must ensure that its systems and data are secure.

Over the past few years, we have conducted a number of reviews in accordance with the Federal Information Security Management Act of 2002 (FISMA). These reviews have shown that while SSA is in general compliance with FISMA, additional steps must be taken to achieve full compliance. These reviews assist agency managers in addressing the challenges of systems security. They also provide the Administration and Congress with useful information regarding agency efforts to secure their information systems, including sensitive data and operations.

Further, our annual Financial Statement Audit tests security controls that SSA has in place to protect its information. These tests range from reviewing configuration settings on the Agency's computers to penetration testing against the Agency's firewalls. In past years, our financial statement audits have identified improvements the Agency needs to implement to ensure the protection of its information. For example, we identified a reportable condition related to weaknesses in areas including access control, security monitoring, suitability and continuity of operations. In response, SSA has worked diligently to resolve the issues that generated the reportable condition. Some of these issues have been resolved. The Agency is working to resolve the remaining open issues.

What remains to be done

SSA must remain vigilant to ensure the integrity of all of its data. OIG works closely with SSA to help meet these demands through detailed audits of Agency efforts and careful investigations of specific attempts to breach security in its systems. With wireless technology already widespread and greater potential for its use on the horizon, SSA and all Federal agencies must make certain that there are proper safeguards in place to prevent unauthorized access where these devices are used. With more applications connecting to the web, it is essential that authentication processes are sound and that SSA knows for certain it is communicating with the right person. SSA must continue to strike a balance between the need to be user-friendly and the demands for increased security.

Together with Congress and SSA, we have made important strides in reducing vulnerabilities, and that effort continues. Since SSA's inception, it has maintained a robust program for protection of the personal data it holds in trust for our citizens. As technology has advanced, SSA has kept pace in developing appropriate safeguards against intrusion.

Still, to strengthen our defenses even further, we believe SSA should work with agencies across Government to improve safeguards for data security. We also believe SSA and lawmakers should examine the feasibility of the following initiatives.

- Limiting the SSN's public availability to the greatest extent practicable, without unduly limiting commerce.
- Prohibiting the sale of SSNs, prohibiting their display on public records, and limiting their use to legitimate transactions.
- Enacting strong enforcement mechanisms and stiffer penalties to further discourage SSN misuse.

Conclusion

We appreciate the invitation to speak with this subcommittee and help inform the very important work you do to protect computer systems, information and data from the threat of cyber attacks, electronic data theft and other security breaches. We will continue our vigilance in addressing these issues and stand ready to do more to enhance the safety and well-being of all Americans. I would be happy to answer any questions you may have.

Thank you.

Mr. PUTNAM. Thank you very much, and I want to thank all of our first panel of witnesses, and we will go straight to questions.

Commissioner Swindle, in the current threat environment in which we live where systems face ongoing attacks, probes, or are constant for vulnerabilities, the bots, the zombies and everything else, some companies, it is becoming clear, are purposefully avoiding conducting IT risk assessments because of the fear that those assessments themselves will establish knowledge of vulnerabilities that could be used against them in litigation. What are your thoughts on the position that a lot of these companies have taken?

Mr. SWINDLE. Mr. Chairman, I would compare their conduct to that conduct you spoke of earlier about lawyers recommending they don't have privacy policies so as to avoid liability. I think it is a road to suicide, quite frankly, because it will catch up with them eventually. And, I think consumers, as they become more aware of the full privacy issue and certainly information security issue, are going to look to companies that are responsible, and they will and turn away from those that are not. Soon there will be more of those that are resonsible than not, and the losers will be the ones that choose this course of action. I think it is incredibly dumb.

I have encountered this in several fora that I have attended over the years, and I just look at them with astonishment that they would take that approach, because I don't think it is realistic. It is certainly not responsible.

Mr. PUTNAM. Is there a need for some form of safe harbor that would encourage companies to conduct thorough examinations and then come forward with whatever deficiencies they find?

Mr. SWINDLE. Safe harbor, I would say, is perhaps a good vehicle to protect those who do the right thing, and inadvertently have security failures, as I said, no security package is going to be complete. They have taken responsible actions, they have done as much as they could see to do, and a breach occurs—I don't think they should be held responsible for something they couldn't really avoid. But, I have a hard time giving people an easy way out, if you will. But, we may have to come to that position, because, as both Mr. Clay and yourself have mentioned, these problems are growing.

We are making progress, but the problems are growing faster oftentimes than the progress, and it may be that we have to seek some kind of means to encourage people to get in and start doing the right thing. But, I would still prefer to see the private sector lead, for their own self-interest, to do the right thing. I am still not convinced that we are incapable of doing that. I have hopefully not unfounded confidence that we will do the right thing.

Mr. PUTNAM. Thank you.

Mr. Martinez, Mr. Johnson, a recent survey was conducted by Carnegie Mellon and Information Week of 100 small and medium-sized businesses that found that 17 percent of the participating companies had been the targets of some form of cyberextortion. Could you tell us more about the cyberextortion problem and the trends that you are seeing out there, and what advice you would have for companies who are faced with that threat? With the FBI?

Mr. MARTINEZ. Well, in simplified terms, the cyberextortion is not just the mere use of the facility of the Internet to make an ex-

tortion as demand, but instead a sophisticated hacker might find a vulnerability in a system, steal proprietary information, customer lists, personnel information from a company, and then pitch them that they can fix it. And if they aren't allowed to come in as a, "consultant," they will release that information in a way that would be harmful to that company. That's one manner in which it can occur.

Trends, the level of sophistication, absolutely is going up. The ease with which tools can be obtained to make the initial intrusion are becoming far, far more available and simpler to use. It doesn't take a rocket scientist to drive some of these tools at this point. It was mentioned previously about the playing field changing from hacking for fun to now hacking for profit.

As far as advice goes, of course, good computer security, engaging in private industry partnership, partnerships with law enforcement organizations such as InfraGard where information could be shared so that we can have a prophylactic effect, you know, share information about how we can protect systems, and also, as was mentioned previously, have a response plan. Companies have to have a response plan, they need to know what to do when they have been attacked. By all means, contact law enforcement.

There's a lot we can do. There are a lot of resources we can bear to solve the problem. Not all of these problems can be solved from the desk, from the desktop of a systems administrator.

Again, we need to know how to respond, how to freeze evidence, how to establish the logs so that we can go in and determine what the methodology was, see if it is common with another case we have been working in the past and what resources we can bring to bear to work with the problem.

Mr. PUTNAM. Mr. Johnson, I understand that the Secret Service recently released a report on insider cybercrime activities in the banking and finance sector. As part of its ongoing insider cyberthreat study, could you elaborate on the threats of that study, the difficulties of dealing with an insider threat, and the implications that report has for combating identity theft?

Mr. JOHNSON. Yes, Mr. Chairman. I echo the sentiments and statements of the FBI in that we recently had a case involving AOL that involved an insider threat, the selling of personal identities to spammers for monetary gain.

With the insider threat, the last 2 years, the Secret Service, in conjunction with Carnegie Mellon University CERT Coordination Center, collaborated on this insider threat study. The threat to critical systems includes individuals who have manipulated vulnerabilities within the system for personal gain, as is the case I mentioned with AOL. Some of the relevant findings of the study were similar to a lot of things that we have talked about today, and that is updating firewalls when employees leave, taking them out of the access to networks, changing passwords. The simplest-type things are being overlooked by businesses and IT people.

Most incidents were not sophisticated or complex. A majority of the incidents were thought out and planned in advance, and, in most cases, others had knowledge of the insider's intentions, plans and activities.

Like the locks on your doors, changing access to network and changing passwords and updating firewalls is a smart business practice.

Mr. PUTNAM. Mr. Martinez, you mentioned a series of ongoing investigations that involve, in some, the theft of 30 million credit card account numbers and potential losses of $15 billion.

Can you elaborate on how thefts like this grow to such epic proportions, and are the penalties for cybercrime under the current code commensurate with the damage that is being done?

Mr. MARTINEZ. Well, of course, a case can be taken to this scope by consolidating like cases, and that's one of the things we try to do in developing strategies both for proactive efforts, and then also once we have complaints that have commonalities. And in order to do that, we have to employ analytical tools and analysts in a form like IC3 in order to determine if we have a problem that goes beyond the scope of a single complaint.

In this case a rather large list of credit information was obtained. Again, it involved many different credit card companies, and so, again, I think we put the number at 100 that were affected, financial services and institutions.

The idea here is to identify the scope and then work with these institutions, work with victims in order to track back. Let's see where this threat came from, see if we can't put our resources together in order to address the problem and to be proactive about the next attack.

Mr. PUTNAM. Mr. Johnson, do you wish to add anything to that?

Mr. JOHNSON. Not at this time.

Mr. PUTNAM. Very good. My time has expired. I will recognize the distinguished ranking member, Mr. Clay, for his questions.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. Swindle, since your agency carries the responsibility for protecting the private information of consumers, what additional efforts need to be undertaken by FTC to further educate the public and corporate community on issues surrounding identity theft, or is education and awareness the key to prevention, or are more stringent regulations concerning privately held consumer information necessary to improve security?

Mr. SWINDLE. Mr. Clay, I would hope that we are not, as stated, responsible for protecting the privacy of all the American citizens. That would be a hell of a big job, and I know you didn't mean it exactly that way.

Mr. CLAY. I would want you to.

Mr. SWINDLE. We certainly do the best that we can, and we are taking every step we possibly can, given the resources we have—and this is not a plea for more resources, by the way—to help educate, and, through education, to deter the invasions of privacy and this theft of this personal identification of which we have all been speaking, and the damage it can do to people.

A part of an education process is dealing with businesses, it is dealing with government agencies, it is dealing with Members of the Congress, asking them to help us make more people, the consumers, aware. It is dealing with the business association and working internationally, dealing with cross-border fraud issues and trying to work with just hundreds of agencies.

We are now, with our identity theft complaint clearinghouse, I believe we call it, we are making that available to in excess of 1,000 law enforcement agencies around the country. We are about to make it available to the Canadians on a 24-hour basis. We are working with international groups. We are working with local and State law enforcement agencies.

So, there is a lot going on, but I think that gets to the problem, as the chairman had mentioned, and Mr. Clay, I believe you mentioned also, the occurrence of these crimes seem to be growing no matter what we do. And, it is the proverbial needle-in-the-haystack operation, except that this haystack is the global haystack, and there are lots of needles in there. Trying to find solutions and punish those who are guilty is a difficult process.

I don't know that we can solve the problem without massive education of customers and business. Then everyone who is involved becomes aware of the role that they can play and take it seriously. It is going to take a lot more effort. We have some, if I remember correctly, about 45 or 50 Congressmen, that have participated with a program we tried to initiate 2 years ago. We could get what, 395 more that could do it and help us a lot. It is just a massive problem. It is going to take repetition, repetition, repetition.

Mr. CLAY. What are the main things that the public should be aware of? What should they look out for? What advice do you give the public about identities?

Mr. SWINDLE. Well, just starting off, liken it to an automobile. We know automobiles and safety intuitively. We have to get the use of computers into that mode of thinking. That means first realizing that a computer is a very sophisticated thing. It is now just second nature to log on and talk to somebody halfway across the world. When you and I were growing up, we didn't know how to talk to the community 15 miles away.

Things have greatly changed. We have to educate people to learn. It will literally take an education program that starts with young persons. We are not doing enough. But also in the business side of the world, it's talking to businessmen and board members. They have to take information security and privacy seriously. It is their corporation, their business. It should be a primary part of the culture of that company to do these things right, and then it has to ripple right down the stream to the lowest levels.

Mr. CLAY. Thank you for that response.

Let me shift real quickly to Mr. Johnson, and seeing my time is short. It seems to me the responsibility of the Secret Service runs concurrent to many other law enforcement agencies at all levels of government. Can you update us on any specific identity theft prevention activities among groups collaborating with the Secret Service, such as the Joint Terrorism Task Forces or Operation Direct Action? And are these groups improving the methods used to coordinate against suspected identity theft activity?

Mr. JOHNSON. Yes, Mr. Clay. The Secret Service prides itself in the education of local and State law enforcement. We have a Secret Service e-information network that is available on line. We have a CD-Rom for State and locals. We have best practices for seizing electronic evidence.

Operation Direct Action is working with third-party processors. Two of the primary third-party processors of credit cards are involved in Omaha, Nebraska, and Columbus, Georgia. By working and having agents assigned to those locations, we've found that access to the information that they can provide gives us quick response to State and locals or first responders to either identity theft or credit card fraud. We have seen the benefits in a good percentage of the cases that are ongoing and other cases that have been concluded.

Mr. CLAY. I thank you for that response.

And thank you, Mr. Chairman, for your indulgence.

Mr. PUTNAM. You are very welcome.

Mr. O'Carroll, you mentioned that in your work on behalf of the President's Council on Integrity and Efficiency on controls over Social Security numbers that 9 of 15 inspectors reported that their agencies had inadequate controls over the protection of Social Security numbers in their data bases. Given the extensive information security requirements for Federal agencies under FISMA and GISRA, how can this be?

Mr. O'CARROLL. Mr. Chairman, historically the use of the SSN was the Federal identifier of employees, and much as we found with universities where it was on their identification card, in many Federal agencies it was on the identification card for the agency. It was posted on walls. Instead of system security flaws on it, it was mostly posting an easily observable SSN.

And what we are fearing—we did the study of other inspector generals on this thing—is as much as you said there, is our feeling is that the first place to start correcting the use of the publication of SSNs is within the Federal Government. One of the ways that we just changed it recently, as probably many of the people in the room are aware, is when any check was going out from the Federal Government, in the window of it, it had the Social Security number of the individual receiving the check. These are all baby steps that were taken. We finally have gotten that taken off of the check. We have been stopping the publication of it.

We are doing studies now in terms of the uses of non-Federal agencies' use of SSNs, for example, colleges and universities, and we are trying to do an education program to get the SSN taken out of the daily usage. And we figure that will be a good way to prevent its misuse in government, and misuse period.

Mr. PUTNAM. Many companies avoid reporting security breaches due to the effect that the news would have on their reputation. Is that sound policy? It's certainly to a degree understandable. Or does it merely make the problem worse and encourage those cybercriminals by having them to believe that they won't get caught? We'll begin with Mr. Martinez.

Mr. MARTINEZ. Well, this issue is addressed across the board in some of the cybercrime matters that we address. I know when I was an assistant special agent in charge in Los Angeles, we worked with the entertainment community on IPR issues, intellectual property rights, and there was a bit of a dance that we had to do with the industry because they don't like to admit that they have a problem. It is bad business sometimes. It gives their competitors

possibly an edge. And the same thing applies to e-commerce businesses, etc.

So our approach to that is to try to engage to the fullest extent we can with those businesses, give them a comfort with us, let them know what to expect through training. Again, our InfraGard program, that's part and parcel, is to let them know what to expect if they do report and the FBI shows up, what we are going to be looking for, what we would hope to find when we get there as far as the procedures they've put in place to maintain evidence.

Mr. PUTNAM. Anyone else want to answer that? Commissioner Swindle?

Mr. SWINDLE. I believe I addressed this in part in my last response. There is almost a Washington, DC, ostrich syndrome that I think permeates the whole society that when we do something wrong, we fear addressing it up front more than I think is necessary. I think if we deal with things direct, up front, get it out, find a solution, we are far better off. I think it speaks well to the reputation of legitimate companies that they will do that. To do otherwise is just ignoring a problem that will never go away. It will come back, it will be found out, and then you are going to deal with why you covered it up.

Mr. PUTNAM. It is not just Washington, as it might be a network problem, too.

Anyone else want to add to that?

The President has transmitted to the Senate the Council of Europe's Convention on Cybercrime. Given the international nature on this, and we certainly have law enforcement represented has to operate across borders, how important is the ratification of this treaty to improving our ability to apprehend cybercriminals? Mr. Martinez.

Mr. MARTINEZ. Well, absolutely it is important. The FBI has made a significant investment in international training and trying to work jointly with law enforcement agencies in other countries where we know we have problems and issues, where attacks are generated, where phishing schemes are located. And, again, we are very proactive about that, offering through international law enforcement academy several different blocks of cybertraining, ad hoc training really, anywhere in the world where it's required. We have 47 legal attache offices, about to add 3 more, and that's a big part of their job is to put us in contact with law enforcement agencies that need that kind of help.

So having those kinds of devices to allow us to solidify those relationships, standardize the law and response in areas across the world is critical to our being able to address the problem here in the United States.

Mr. PUTNAM. Mr. Johnson, do you wish to add anything?

Mr. JOHNSON. Yes, Mr. Chairman. I would agree and the Secret Service would agree that the victimization of Americans and of businesses overseas is growing at a rapid pace. The world is borderless. The Internet provides the foreign criminals easy access to the United States and their citizens by quickly getting on line. Many countries have Internet access, they have TV access. Foreign public can only buy Western products on line. That is their only capabilities. The growing number of significant investigations over-

seas, virtually all terrorist investigations have a foreign nexus. The field offices that we have established have provided rapid response overseas and provided that capability, and it is also extending the reach of American law enforcement in general.

Mr. PUTNAM. Commissioner, this is my final question, and then I will yield back to Mr. Clay. California has a law that took effect in 2003 that requires businesses or State agencies that maintain computerized data that includes specified personal information to disclose any breach of security to any California resident whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person. What effect do you think that law will have on improving information security? And what are your thoughts on taking it national?

Mr. SWINDLE. Mr. Chairman, as I mentioned in my testimony, there certainly are circumstances where a person ought to be notified that there has been a breach. However, I don't for a minute believe that in every circumstance they should be notified. And I think, taken to extreme, that could be an enormous burden on businesses, and it would solve no problems. I don't think it necessarily would prevent it from happening again, and there may very well not be any damage done at all. A lot of the information that it is personally identifying is publicly known in phone books, for example.

So I think you would have to deal with those circumstances on a case-by-case basis. And, to my knowledge, I think California is the only State, at least to date, that has that kind of legislation. That's not to say it is probably not being considered by many other States, but I think I would move in that direction extremely cautiously because I think it could be an overkill.

Mr. PUTNAM. Mr. Clay, you are recognized.

Mr. CLAY. Thank you, Mr. Chairman.

I will start with Mr. O'Carroll. Since the release of the 2003 report on the internal control structures for the use of Social Security numbers among Federal agencies, have there been any notable improvements reported by agencies that were identified as having deficiencies in the methods and practices used for protecting Social Security numbers or identifiers?

Mr. O'CARROLL. Mr. Clay, we were going to be doing another followup audit on that next year to see what improvements there have been. But anecdotally, from other inspectors general and from having conferences with them and discussions with them, most of those other agencies have all started robust plans on correcting the use of SSNs in their agency, and we expect it to be a much better audit when we do it next year.

Mr. CLAY. Thank you for that.

Let me ask Mr. Martinez. Last Friday the Washington Post published an article on the increasing number of fraud-related investigations by the FBI within the mortgage marketplace, and identified my home State of Missouri as a so-called hot spot of activity. Can you provide for us any information on the number of cases that are specifically related to the use of fake identities or straw buyers or forged loan documents in the recent upswing of activities? Are you familiar with it at all?

Mr. MARTINEZ. I am familiar with the article and the circumstances; and that would fall under the responsibility of our Criminal Investigative Division that has the responsibility for traditional white-collar crime cases. I can tell you that it is certainly within the realm of possibility that type of criminal activity could be part and parcel of mortgage loan fraud. Again, identity theft might very well be applied.

I mean, I think the answer here is that smart criminals will figure out a way to make it work for them. And with this vulnerability, it is just another vulnerability to be exploited, and I think it could be applied. But I couldn't give you specific figures, but I can certainly talk to the Criminal Investigative Division and get back with you on that.

Mr. CLAY. Thank you for that.

Let me ask you for one last question. Can you cite for the committee specific areas where legal or policy barriers continue to impede information sharing or cooperation among stakeholders investigating potential identity theft activities?

Mr. MARTINEZ. I am not aware of any legal impediments. I think there is just an awful lot of work to go around. So the approach we have to take is to just leverage resources. Again, I am not here with my hand out saying we need more bodies. Of course I could throw another thousand agents at the identity theft problem, and in cybercrime in particular, and not solve it and not make a significant dent in what might continue to be the problem.

But that said, we do have many, many initiatives that are intelligence-based. I've mentioned IC3 several times. It is more than just a place to receive complaints. We take that information, we crunch the numbers, we decide where can we apply our resources, our cyber task forces' resources, State and local resources that can be brought to bear, regional forensic labs to address the problem.

So it is enormous, but I do think that with some collaboration, with our partners especially, you know, we have mentioned several times with private industry, it is enormously important. We can't do this alone. They are often out in front of us as far as being able to detect and plan and see threats coming. So we need to continue to leverage those resources the best we can.

Mr. CLAY. How successful is your agency in apprehending those who participate in identity theft, those—especially the bigger fish so to say? Pretty successful?

Mr. MARTINEZ. Well, I guess I would like to say that we have had some tremendous successes. Some of the things that impede those successes are, again, the international nature of the problem. Some of the groups that are perpetrating these types of crimes are located in countries where we don't have a good established working relationship. We work awful hard at it, but there is just—sometimes you can't overcome those problems. But, again, it is something that we need to work at every day. We do have a good network of legal attache offices and training and outreach that goes toward making those kinds of strides.

Mr. CLAY. Thank you for that response, Mr. Martinez. I yield back the balance.

Mr. PUTNAM. Thank you, Mr. Clay.

Before we wrap up this panel, I would give all of you the opportunity to have a final word or answer a question you wish you had been asked, whatever the case may be. And we will begin with Mr. O'Carroll and go down the line and just give you a moment, if you have anything that you would like to say, and then we will seat the second panel.

Mr. O'Carroll.

Mr. O'CARROLL. The only thing I have to add, Mr. Chairman, is—continuing on with what Mr. Martinez said, is that I think nowadays since we all have so much more work than we have people to handle it, that the wave of the future is going to be cooperation between all Federal law enforcement agencies and also working with local agencies. And by doing that, we are using the task force concept which is being used right now very effectively in the terrorism arena.

In the identity theft arena, I think that is the solution. We can share information, it is easier to do it, there is less structure—or strictures in relation to disclosures of information on a task force. And I think that is something that we are going to be seeing a lot more of. We participate in about six identity theft task forces around the country that have been very successful.

Mr. PUTNAM. Mr. Johnson.

Mr. JOHNSON. In closing, Mr. Chairman, I would agree with Mr. O'Carroll, that our Electronic Crimes Task Force is—the 15 that we have established, we are looking to double that number in the next 3 years. To further Mr. Clay's earlier question to Mr. Martinez about the big fish, are we—I would just like to say to the chairman that the Secret Service is, through prevention, our training at the local levels all the way up to the disruption of the major players in financial crimes and identity theft, that we are making inroads every day with these investigations. That along with the Electronic Crimes Task Forces in the United States, the Secret Service is not only dedicated to the problem, but it is a priority of our agency.

Mr. PUTNAM. Thank you.

Mr. Martinez.

Mr. MARTINEZ. First, I want to tell you how much I appreciate and the FBI appreciates the opportunity to come and speak to you today and talk about this important crime problem. And I want to tell you how much we appreciate Congress' support in enacting the SLAM-Spam Act, the identity theft penalty enhancement. These are the types of real tools that we can go out and take and try to make an impact on this crime problem. I just appreciate the opportunity to speak to you today. Thank you.

Mr. PUTNAM. Thank you, sir.

Mr. Swindle.

Mr. SWINDLE. Mr. Chairman, someone, I've forgotten whether it was you or Mr. Clay, asked the question to another participant about whether or not the penalty matched the crime. I have been a Federal Trade Commission for roughly 6½ years now, and one of my great frustration is to see one scam artist after another come through our process. Our staff does remarkable work in finding them, building the case, but we are a civil penalty organization and do not have criminal authority. Oftentimes we find we catch the spammers, we catch the scam artists, and so much of it is being

done electronically now, and we expend great resources to get them, and they have nothing. It is just a difficult task. I don't think the penalties anywhere come close to matching the crime.

One of my greatest frustrations is that it appears as though some of this conduct is almost just the price of doing business when you get caught because the penalty is so insignificant relative to the size of the profits made.

Another one is oftentimes we find people after we track them down and they have ripped off the consumers for multimillions of dollars. Guess what? They have no assets except perhaps a million-dollar house in Florida which we can't touch because of the homestead exemption. We ought to find ways to adjust the laws so that you don't get homestead exemption if you are engaged in criminal activity or alleged criminal activity and you settle.

It is a big problem. I think it is demoralizing to those who try to apprehend these people, not to mention the poor victims of some of these crimes, which it is in staggering proportions. And I think that is something we should seriously look at.

Mr. PUTNAM. Thank you very much. I want to thank all of you. And at this time we will dismiss panel one, and the committee will recess for such time as it takes to set up the second panel.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene. I would like to invite our second panel of witnesses and anyone accompanying them to please rise and raise your right hands for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all the witnesses responded in the affirmative.

We will move directly to testimony beginning with Howard Schmidt. Mr. Schmidt joined eBay as vice president and chief information security officer in May 2003 after retiring from the Federal Government with 31 years of public service. He was appointed by President Bush as the vice chair of the President's Critical Infrastructure Protection Board and as the special advisor for Cyberspace Security for the White House in December 2001. He assumed the role of the Chair of the Board in January 2003 until his retirement in May 2003.

Welcome to the subcommittee. You are recognized, sir, for 5 minutes.

STATEMENTS OF HOWARD SCHMIDT, FORMER WHITE HOUSE CYBERSECURITY ADVISOR, AND VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER, eBAY, INC.; BILL HANCOCK, VICE PRESIDENT, SECURITY PRACTICE & STRATEGY, CHIEF SECURITY OFFICER, SAVVIS COMMUNICATIONS CORP.; BILL CONNER, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, ENTRUST, INC.; AND JODY WESTBY, CHAIR OF PRIVACY AND COMPUTER CRIME COMMITTEE, AMERICAN BAR ASSOCIATION, SECTION OF SCIENCE AND TECHNOLOGY LAW, AND MANAGING DIRECTOR, PRICEWATERHOUSECOOPERS

Mr. SCHMIDT. Thank you, Mr. Chairman and Ranking Member Clay. Thank you very much for the opportunity to be here today.

I would like to keep my verbal comments relatively brief in lieu of all the questions that you had last time and I am sure you will have again. But I want to basically focus my remarks in three major areas: One, what eBay is—the company itself is doing relative to the leadership, relative to the area of on-line identity theft and phishing, as you have cited to, accurately so, a growing threat to consumers, business, Federal employees, and basically anybody that uses the Internet; also, some of the industrywide efforts that are taking place to collectively combat this area; and then some thoughts I think that I want to share relative to the public-private partnership that is so crucial to our success in moving forward on the cyberspace security area, but more specifically on the on-line identity management.

You know, you have heard the numbers from the FTC. They reported earlier this year that the identity theft topped the list of consumer complaints for the 4th year in a row, about a 33 percent increase in what we have seen over the previous years, and even that didn't tell the full story. In June of this year, the Forrester Report showed approximately 9 percent of U.S. on-line consumers, about 6 million houses that use the Internet, that experienced identity fraud. Now, when you look at the overall international user base on the Internet, it is estimated to be about 840 million users currently. So we are talking about just the U.S. portion of that. And what I probably worry about most more than anything else is the fact that the numbers that we have mentioned are potentially capable of growing if we don't take action quickly and we don't move in a cohesive measure between private sector and public sector.

One of the reasons, of course, as some of the previous folks testified about, and that is this issue around phishing. What we have seen is an evolution as we have been very, very concerted about better cybersecurity for enterprises. You mentioned the California 1386 law relative to reporting things, Sarbanes-Oxley-Graham. You list the name of things that have given us incentives to do things better when it comes to cybersecurity, and corporations both publicly traded as well as privately owned are doing more. We are starting to see the shift, the attack factor shift to the less sophisticated, the end users, the cable modem users.

You know, we have seen instances even recently where phishing e-mails have come reported to be from the FBI, the FDIC telling people that if you don't fill out this form and give us all your information, Social Security number, mother's maiden name, dog's name, address, high school, we are going to shut down your bank account, and that is tremendously scaring to the uneducated and the non-IT professional.

But it is interesting that this is not a new phenomenon. We have been dealing with this for over 20 years. In the 1980's, we were actually teaching classes at the Federal law Enforcement Training Center in Georgia on what we called at that time carting, with actually doing shoulder surfing, going to airports, New York La Guardia, and looking at people as they used calling card numbers and credit card numbers to make calls and using that for identity theft. And what we have seen as of about 2 or 3 years ago when this new spate of phishing started, they actually started from a

perspective of trying to grab on-line time for free. It wasn't about identity theft, it wasn't about credit card fraud, it was getting on line for free.

And then what happened is that evolved, and they said, well, listen, we can make money off of that. And I think all the previous witnesses testified as well that this has now moved from clever hobbyists and people thinking they are being funny and hacking to where it is true criminal enterprises. And other reports came out this year that estimated 57 million users on line had received phishing e-mails. I am averaging one a day now from major institutions all around the world.

Mr. PUTNAM. Excuse me. Can I just interrupt? Does that include the Saudi plea?

Mr. SCHMIDT. Yes.

Mr. PUTNAM. Because that has to be at least two-thirds of it.

Mr. SCHMIDT. That is a big chunk of it. Absolutely correct. And then, of course, we add into the political fundraising portion of it as well. And what happens now, we are seeing a more focused, what is being referred to by Marcus Jacobson, who did some analysis while at RSA Security Laboratories, what they call context attacks, where the phishing attacks are the same way. You just recently bought a new car, here is information relative to that, and really convincing you that this is a legitimate e-mail. So consequently, you know, this is indeed a new challenge we have not seen before.

Now, what are some of the things we are doing? One, first and foremost, many of us, particularly those of us who have multi-multi-million-user bases like we do, are doing a continuous education process. We've changed our business process, so we no longer send active links in e-mails that we send to customers anymore. As a matter of fact, we tell them, if you want to do a transaction, type in the URL or use a bookmark. But basically we have also spent a tremendous amount of resources hiring people to do full time where we have the ability to identify these phishing sites on a near real-time basis and take them down.

Now, in closing, I just want to make one quick comment relative to the overall homeland security piece, because as we were doing the national strategy to secure cyberspace out of the White House, some government agencies didn't feel that identity theft and identity management were homeland security issues, and I truly believe they are.

One, first and foremost, no better tool—as we get better about physical identity, no better tool than for a terrorist or an organized crime to use—criminal person to use than your good name to be able to assume your identity and be able to pass through airports. Second, it becomes a nexus. And as you see in my written testimony that we are seeing 30,000 users that are being compromised on a regular basis that then can be used to launch denial of service attacks. And, last, to become a gateway into corporate enterprises such as critical infrastructure. And it is important to make sure that we do everything we can to stop that from taking place.

So, with that, I thank you for the opportunity again, and I stand by for any of your questions you may have. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Schmidt follows:]

TESTIMONY BEFORE THE

GOVERNMENT REFORM SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

U.S. HOUSE OF REPRESENTATIVES

September 22, 2004

By Howard A. Schmidt
Chief Information Security Officer, eBay Inc.

Introduction

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

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

I continue to proudly serve in the U.S. Army Reserves, assigned to the 701st MP Group, (CID) as a Special Agent with the computer crime unit at CID headquarters. I also serve on the Board of Directors for $(ISC)^2$, the body that oversees certification of security professionals through the CISSP certification. And, I serve on the Information Security Privacy Advisory Board, appointed by the Secretary of Commerce to advise NIST, CSD and OMB.

The challenges of identity theft and ID management

My remarks today will focus in three areas: 1) how eBay has been one of the leaders on the issue of online identity theft and "phishing," a growing threat to consumers, businesses, federal employees and basically anyone who uses the Internet; 2) an overview of some of the industry wide efforts that have been undertaken to combat online ID theft; and 3) a discussion of some steps that the public and private sector can work on to move forward in providing online identity management.

You have probably heard some of the numbers before. The U.S. Federal Trade Commission (FTC) reported earlier this year that identity theft topped the list of consumer complaints for the fourth year in a row. Unfortunately, online fraud accounted for a large number of these complaints. The FTC received 33 percent more identity theft complaints in 2003 compared with 2002, and Internet fraud accounted for 55 percent of all fraud complaints, up from 45 percent in 2002. These numbers alone don't tell the full story. According to a June 2004 Forrester Research report, nine percent of U.S. online consumers – 6 million households that use the Internet – have experienced identity fraud.

What's both interesting and troublesome about the numbers that I just mentioned, including the large number of households that have been victimized by online criminals, is that the numbers reported by the FTC next year are likely to be worse if we do not take action now. Why? One major reason is the explosion in phishing scams on the Internet. Phishing, or the use of fake e-mails and Web sites to steal bank account and other sensitive information such as social security numbers, has "hoodwinked" millions of victims globally. The criminals send thousands of emails telling people that there is an error with their online account and ask them to fill in an "update form" or their account will be closed. This form has the look and feel of major e-commerce sites – there was even a fake email from someone pretending to be the FBI and the FDIC asking unsuspecting users to enter personal information into a fake web site or their bank account would be closed. While online criminals have been busy, they have also been quite successful.

Although this appears to be a recent phenomenon, identity theft is a very old type of crime. The "phishing" email is but a new twist to an old scam. In the mid 1980s we taught classes at the Federal Law Enforcement Training Center on a technique called carding, where individuals would "shoulder surf" people's credit and calling cards at airports and train stations, then distribute them worldwide via "Computer Bulletin Boards." Dumpster diving still is an effective method for individuals to obtain personal information and is used regularly to create false identities. Hacking into systems and stealing personal information is yet another way this disturbing trend is continued. As we get better at securing our systems, as online security improves, the next "soft target" the cyber criminals go after are the end users, relying on age old methods involving scams and deception. This is the basis of what "phishing" is all about. Some of the first instances of what we now call "phishing" started over 5 years ago when individuals sent fake emails reporting a problem with an account, and presented a "form" to fill out and

"fix" the account. The initial intent was to steal online time from legitimate users for criminals' use. This has since changed to be mainly a financial motive.

According to a June 2004 study by Gartner, nearly 2 million people reported that their checking accounts were breached in some way during the last year. In a May 2004 study, Gartner reported that a staggering 57 million online users in the United States alone had received a "phishing e-mail during the prior year. Gartner reports that direct losses from identity theft fraud as a result of "phishing" attacks – including new account, checking account and credit card account fraud – cost U.S. banks and credit card issuers about $1.2 billion last year. These numbers are likely just the tip of the iceberg and the impact on our economy as well as our pocketbooks is considerable.

Why are consumers and businesses being duped? Well, many of the reasons tie into social engineering. But, not all of them. Heightened awareness alone will not stop "phishing". Better cyber hygiene is surely a part of the solution, but it is only one important part. The reality is, as more people become aware of current "phishing" scams, the cyber criminals often get even more clever, and create new, more sophisticated techniques. One example of an emerging threat in phishing is what a colleague at Indiana University calls "context aware" "phishing" attacks. These attacks are mounted using messages that are somehow expected (or even welcomed) – from their context – by the victim. Markus Jakobsson, who started his analysis of this problem while a Principal Research Scientist at RSA Security Laboratories in Massachusetts, states that initial analysis of context aware attacks indicate a success rate of close to 50 percent. *Note: See "Modeling and Preventing Phishing Attacks" by Markus Jakobsson, School of Informatics, Indiana University at Bloomington.

Corporate enterprises such as eBay are continually enhancing security. But new threats require continued education of the end-user, technology improvements, information sharing and analysis to reduce the impact of these threats. eBay has developed advanced applications to identify potential spoofed/"phishing" web sites and has established a full time team dedicated to identifying and taking down these spoofed/"phishing" sites as well as notifying other companies when spoofed sites are discovered. Working with our partner Whole Security, Inc. eBay has also created an account guard feature within the eBay toolbar that turns green when on an eBay or PayPal site, and turns red and displays a dialogue box identifying it as fraudulent if one goes to a phishing site. If an eBay password is used on a site that is not eBay, the account guard feature displays a dialogue box stating that it is not a good practice to use the same password for multiple web sites. eBay continues to work with other industry leaders looking for long term solutions to identify theft and "phishing."

What Can Consumers and the Public and Private Sector Do?

The widespread success of current phishing and other kinds of online fraud combined with criminals constantly coming up with more sophisticated ways to scam, means that Internet users have to do more. One critical first step is authentication. While

putting together the *National Strategy to Secure Cyberspace* I emphasized that authentication had to be included. "A/R 4-2: Through the ongoing EAuthentication initiative, the federal government will review the need for stronger access control and authentication; explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms; and, consequently, further promote consistency and interoperability."

Think about it. To know that you are you is really important to your online commerce auctioneer, your online store, your bank, your DMV, your online pharmacy, the IRS...you get the picture. And, if you think about it some more, strong or two-factor authentication methods are the best way to protect your identity and your personal, business, or government agency information. When drafting the *National Strategy to Secure Cyberspace* the concept of strong online authentication was not viewed as a Homeland Security issue by some offices within the government. But I contend that it is a Homeland Security issue. The lack of strong online authentication allows an individual's private information to be accessed by unauthorized persons who can then take over that individual's good identity. Computer systems can also be taken over and used in concert with thousands of others to launch distributed denial of service attacks. In recent past law enforcement has seen instances of more than 15,000 broadband connections being hijacked and turned into a remote (bot) network. In many instances end-user machines used for remote access into corporate networks can be compromised, thus also providing a gateway into critical infrastructure. As we get better at protecting physical identification, the next logical place for terrorists and organized criminals to obtain identities is online. We can prevent this by implementing strong two factor authentication.

With the new threats we have seen increasing online, passwords will need to evolve into a more strong method of authentication in the future. Passwords that are easy to remember can be easily guessed by hackers, and passwords that are more complicated have to be written down, making them more vulnerable to thieves. Do you or members of your family use the same easy-to-remember password at multiple sites online? Do you or your employees write your password on a piece of paper and put it under your mouse-pad at work? These are pretty common mistakes and even users that are generally more cyber security aware sometimes make them out of convenience.

We have created a system where we must use complex passwords to login to various systems. We also have to change those passwords frequently creating another challenge for mere human beings to remember these complex passwords. This is made even worse by the need to use different passwords for different systems that few people voluntarily choose to do. This is a known weakness often exploited by criminal hackers.

The government can be a leader in accelerating the creation of digital identity management that would work for government services as well as online e-commerce. The nation could be well served to have two-factor authentication in place by the end of 2005. The DoD has moved this process forward through their Combination Access Card (CAC). Many federal agencies and even security conscious legislatures, including the House of Representatives, use Secure ID smart tokens from the identity and access

management provider RSA Security for remote logical access. The President's Homeland Security Directive on August 27th that establishes a "Policy for a Common Identification Standard for Federal Employees and Contractors" has significantly elevated the use of federal identities as a federal government priority. The Directive requires the new standard being developed by the National Institute for Standards and Technology be implemented by the end of November 2005.

Consumer facing companies have an important role to play as well. My company, eBay, constantly educates consumers about the importance of authentication as well as good cyber hygiene. We believe that we are one of those forward-thinking companies that get it and will continue to offer our users more and more solutions to combat identity theft and other online threats. I am a great believer that federated identities can be recognized as easily as a driver's license, military ID or passport with the extra feature of instant validation online. One example of using federation is to have the ability to log onto my organization's network while using the same federated identification to do my online banking or shopping online from overseas.

Consumers are demanding more security and key players are stepping up to the plate. Companies such as RSA Security, Entrust, GeoTrust and Verisign have been leading this charge for a number of years and now provide solutions for improved identity management not available in the past. Recently a major ISP and RSA Security announced that strong authentication devices will now be available to millions of consumers through an easy to use subscription service. This is a major development and I anticipate that more and more ISPs, banks and other businesses will be taking this very important step in the coming months and years. Consumers benefit, businesses benefit – we all benefit. Criminals lose.

In addition to offering specific solutions, industry is coming together in various groups to educate the public, share information, discuss emerging threats, and address public policy issues related to phishing and other online fraud. We worked with the Information Technology Association of America (ITAA) to pull together a number of providers and vendors – including eBay – to form the Anti-Online Identity Theft Coalition. The Coalition has four major goals: 1) to build technology to reduce the likelihood of these mails ever reaching their intended victim; 2) to provide awareness training to consumers so they can more readily identify these criminal acts; 3) to share information on new scams amongst the various security teams; and, 4) to insure accountability by working with law enforcement to identify and prosecute these bad actors.

The Anti-Phishing Working Group has become a one-stop shop for information on "phishing". Many organizations – public and private – share information within the group about current and evolving threats. The financial services industry has an important anti-fraud working group at BITS and the Financial Services Technology Consortium has a counter-phishing initiative. The National Cyber Security Alliance is a public-private partnership spearheading efforts to educate consumers and small businesses on cyber security and protection from online identity theft.

Another organization working on identity management is the Electronic Authentication Partnership (EAP). This group is a multi-industry partnership working on the vital task of enabling interoperability among public and private electronic authentication (e-authentication) systems. Interoperability of e-authentication systems is essential to the cost-effective operation of safe and secure systems that perform essential electronic transactions and tasks across industry lines.

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

Role of Cyber Crime Investigations

The Department of Justice (DoJ), the U.S. Secret Service and the FBI have significantly decreased their response times and increased the priority of cyber crime investigation. FBI Director Mueller has placed cyber crime as a top five priority of the FBI, and the Secret Service has added a number of electronic crime task forces to investigate and prosecute cyber criminals. All of DoD's criminal investigative organizations are leaders in investigating cyber crimes and include among their ranks some of the best investigators in the world. DoJ, through its Computer Crime and Intellectual Property Section, has chaired the G-8 Subcommittee on cyber crime and has been a significant driving force in combating cyber crime worldwide.

For the past three years, we have seen a significant increase in the number of cyber crime investigations undertaken by all levels of law enforcement, federal, state, local and international. Although we have had success in a number of investigations, I would recommend to the Committee to look again at the federal agencies and their coordination and investigative responsibilities.

Just two weeks ago, the Department of Justice announced Operation Slam Spam in which the private sector, law enforcement, the National White Collar Crime Center and the Internet Crimes Complaint Center took dramatic steps against those that would continue to attack our online personalities. I am assured that this will not be the only strike against those that affect the way we work, play and enjoy the online world.

Conclusion

Despite these and many other efforts, solutions, and security enhancements, we can be certain that the nature and sophistication of online fraud and "phishing" scams will evolve. To combat this evolution we need to quickly move to a world where strong identity is the standard and where we have a greater assurance that we can choose any type of a device, whether it is a smart card device, an RSA secure ID device or a USB device, and we can use it for government and e-commerce.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology-led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work, live, and learn.

I thank you once again for the opportunity to appear before this distinguished committee and I look forward to any questions that you might have.

Biography of Howard A. Schmidt

Howard A. Schmidt joined eBay Inc. as Vice President and Chief Information Security Officer in May of 2003. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003, until his retirement in May 2003.

Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.

Before Microsoft, Mr. Schmidt was a supervisory special agent and director of the Air Force Office of Special Investigations (AFOSI), Computer Forensic Lab and Computer Crime and Information Warfare Division. While there, he established the first dedicated computer forensic lab in the government.

Before AFOSI, Mr. Schmidt was with the FBI at the National Drug Intelligence Center, where he headed the Computer Exploitation Team. He is recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Before working at the FBI, Mr. Schmidt was a city police officer from 1983 to 1994 for the Chandler Police Department in Arizona..

Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard from 1989 until 1998 when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division. He has testified as an expert witness in federal and military courts in the areas of computer crime, computer forensics and Internet crime.

Mr. Schmidt had also served as the international president of the Information Systems Security Association (ISSA) and the Information Technology Information Sharing and Analysis Center (IT-ISAC). He is a former executive board member of the International Organization of Computer Evidence, and served as the co-chairman of the Federal Computer Investigations Committee. He is a member of the American Academy of Forensic Scientists. He serves as an advisory board member for the Technical Research Institute of the National White Collar Crime Center, and is a distinguished special lecturer at the University of New Haven, Conn., teaching a graduate certificate course in forensic computing.

He served as an augmented member to the President's Committee of Advisors on Science and Technology in the formation of an Institute for Information Infrastructure Protection. He has testified before congressional committees on computer security and cyber crime, and has been instrumental in the creation of public and private partnerships and information-sharing initiatives.

Mr. Schmidt has been appointed to the Information Security Privacy Advisory Board (ISPAB) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA), a master's degree in organizational management (MAOM) and an honorary Doctorate in Humane Letters from the University of Phoenix.

Mr. PUTNAM. Our next witness is Dr. Bill Hancock. Dr. Hancock is the vice president of Security Practice & Strategy and the chief security officer of SAVVIS Communications, a large global telecommunications hosting and IT services company. He has designed thousands of networks and has been involved in hundreds of hacker investigations in his career of over 30 years in the high-tech industry.

Dr. Hancock has written extensively on security and networking. He is well known in the industry as a technical visionary due to his various original inventions such as stealth firewall technology and intrusion detection and prevention technologies. Dr. Hancock is also a founding member and immediate past chairman of the Internet Security Alliance.

Welcome to the subcommittee, sir. You are recognized for 5 minutes.

Mr. HANCOCK. Thank you, Mr. Chairman, Mr. Clay, members of the subcommittee. I would like to start off by saying I'm probably the geek that you are going to have to deal with today, and a geek with nervous social skills.

With that, I would like to do—we have heard from everyone today about how bad the identity theft problem is. I would like to do a couple things and point out a couple of little broader topics having to do with identity theft, and then also offer some ideas in terms of correction.

One of the problems that we have with the basic concept of identity is, what is something? And that gets not even to the point of what is money. We often think very much about what happened on September 11. I had friends that were in one of the aircraft that hit the World Trade Center, I have acquaintances that were involved in the Pentagon, and I can tell you categorically that if we suffered a cyberattack against our financial resources of this Nation, it would cause trouble that you cannot possibly imagine. I will say that specifically for this reason: Money is an entry in a data base; it is not a pile of cash in a vault, it is not a bunch of collateral that is spread around evenly throughout different organizations. Anymore when you present a credit card or you go to an ATM machine, and you take that credit card in that ATM machine and you swipe the magnetic strip, everything in the middle assumes that is really who you say you are, and that the person who owns that card and the person that possesses that card is the person who is supposed to have that card.

We know from past experience, and I am sure that other panelists will agree with this, that there are an enormous number of ways to go back and spoof credit cards, to create new credit cards, to go back over and create false magnetic strips and all kinds of other mechanisms. And those things are widely available on the Internet and almost anywhere you would like to go.

Specifically, though, we have other types of attacks that happen because of identity theft because we continue to use protocols which are 30 years old. Specifically, when we sit down and consider the fact of things like denial of service attacks, which can be debilitating over a network, that can take out a complete Website, that can take out e-commerce, that can knock out a company completely from its network presence, what we find is that many times those

attacks are caused by spoofing of source addresses or spoofing of destination addresses because we do not properly identify devices that join the network. If you are a device, and you get on the network and you send the right formatted message, something gives you a TCP/IP address, you are allowed to join the network, and you can go back and do whatever you want to do.

In the cases of things like distributed denial of service attacks, there are literally networks of hundreds of thousands of zombies, and there is more and more being created every day. As a matter of fact, I read an estimate just yesterday morning that says that there is over 30,000 machines a day are being acquired and put into zombie networks. These particular networks can be used to go back and spoof source addresses because we do not adequately identify machines, identify technologies that join the networks, and then those source addresses can be used to go back and debilitate a company that is legitimately engaged in e-commerce all over the network.

So as we go back and we examine identity management, I think one of the things that is very important to understand is that we not only have the problem that we all hear about consumer identity being stolen, that our consumer debt and consumer confidence is being eroded, but simultaneously we are also having the problem that networks themselves are being killed off from the simple fact that we have network technology that is being used that was never developed with security in mind. There are no controls in the TCP/IP protocol sweep whatsoever to go back and deal with the identity of a device that joins the network. There is nothing within the protocol that is used for Web sciences such as XML and HTML to properly authenticate and identify an individual or identify a particular program that may want to go back and access them back in.

As a brief example, one of the more classic things that happens is when a front-end data base that is located on a Web surfer wishes to discuss something with a back-end data base that may be a legacy mainframe, what we find very often is that there is a singular identity that is exchanged between the two data bases. And if you look at every single data base transaction that happens, it comes from that same singular identity no matter who came in on the front end and no matter what you are asking for on the back end. And that is because of improper identity management at the program level.

So, so far we have discussed the problems of identity management at the device level, at the program level. We know of the problems with the individuals.

So, therefore, what kind of things do we need to do? One of the things we need to very seriously think about doing is a heavy lift of different protocols that are used in network communications. This is a very big deal because it allows us to properly identify devices and properly identify services, properly identify applications that are actually transacting over the networks. Eventually security should be invisible. It should be just like you walk in and you startup your car, you put a key in the ignition, and all kinds of magic happens. The fact that there is 28 processors under the hood and there is probably a network running around inside the car is

totally irrelevant to you. And that is the way security should be over time. We can't do that until the protocols themselves have the controls and capabilities built into them.

We need to start thinking about authentication implementation and audit capabilities at all companies. And, frankly, I am more concerned about companies involved in things like power grid management, water networks, food processing, food movement-type of networks, because all of these use the same protocols, all of these have exactly the same problem, yet the level of criticality of these particular networks and these particular types of infrastructures are more critical in terms of what we do.

A good example is air-to-ground, ground-to-air uses a specific set of protocols that are bizarre and unique. Those are all being migrated right now to TCP/IP, which means very soon ground-to-air and air-to-ground communications protocols will be available to Internet connectivity.

We will also find that there needs to be multiple methods of authentication, not just one. And the reason being is that if you compromise one, you don't want to compromise all of them. You need to take the time to establish the different types and different levels of authentication to have a defensive, in-depth type of profile. We need to think about incentives through industry to go back and help people realize that it is a good thing, a profitable thing to instill security, but also to go back over and deal with the identity management problem and to deal with the situation.

We need to take an international approach to all of this, and this may even include modifications of trade agreements to ensure that ourselves, our trading partners and everyone are engaged in proper identity management when we start moving things around between different areas, because the Internet is truly without borders.

And we also need to go back and think about leading from the front. Different companies, different organizations and everything are not incented, they are not told, they are not provided legislative requirements for CEOs to make the proper types of decisions. I deal with this all the time. I go out and I suggest to a customer, please improve your security. And they say, why? And the answer I give back to them as a typical rule is three things: Because of what I call a PAL technique of PR, assets, and the law. There is reasons to protect your brand, there are reasons to protect your assets, and there is laws that you must adhere to.

That tends to be a good business case, but that is not the real reason why people should put in security. They should go back and install identity management because it is the right thing to do.

With that, Mr. Chairman, that concludes my opening remarks. I would be happy to take some questions.

Mr. PUTNAM. Thank you, Dr. Hancock.

[The prepared statement of Mr. Hancock follows:]

TESTIMONY OF DR. WILLIAM HANCOCK, CISM, CISSP
Vice President, Security Practice and Strategy
Chief Security Officer
SAVVIS Communications
before the
House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Hearing on "Identity Related Crime, Solutions and Strategies"
September 22, 2004

Thank you Mr. Chairman. My name is Dr. William Hancock. I am Vice President of Security Practice & Strategy and Chief Security Officer of SAVVIS Communications, a large multinational telecommunications and hosting company. I am Chairman of the National Reliability and Interoperability Council (NRIC) Focus Group 2B, Cybersecurity, a federally authorized council of advisors to the Federal Communications Commission (FCC). I am also the Immediate Past Chairman of the Board of the Internet Security Alliance. I appear here today as a technical expert on the subject at hand on behalf of SAVVIS Communications.

As we have heard from U.S. government experts previously today, identity theft in cyberspace has reached epidemic proportions. Most of this is due to the relative ease in which personal identify information is available on the Internet and via other methods (such as social engineering information from helpful individuals via telephone access to help desks). I believe we can all agree that there is a major problem in identity theft that is only getting worse. Rather than re-hash how bad the problem is, I would like, instead, to focus on what we can do about the issues and pose some potential steps to solve the problems.

Who Has Access to Information is Key

The first problem to come to grips with in the area of identity management is that all information ultimately ends up in a database or data repository of some sort. Identity management is not just about what information is in a database that can be stolen and used for illicit purposes – it's about WHO is allowed access to that information and what rights they have to manipulateit.

As an example, the concept of "what is money" has changed radically since the early 1900's. Originally, an individual's wealth and holdings in terms of finance were based upon collateral wealth, substantiated by precious metals, jewels, real estate or other physical holdings which had value attributed to them in some manner. These material possessions were kept in vaults or secured via legal instruments (in the case of real estate) as a method of verification of wealth. In today's modern society, "money" is an entry in a database at a financial institution. Clearing house companies, through a systematic method of mutual

trust, "tell" each other to modify database entries that are assigned to an individual to credit or debit the database entries as financial transactions are performed.

When an individual slides a credit or debit card in the card reader at a grocery store, the bank accepting the transaction works with a credit card clearing house to authenticate the card and post the transaction debit against the card holder's account in a database being held at another banking institution somewhere on a network. There is no physical movement of assets, like gold or jewels, between institutions. There is no signing over of real estate. The entire transaction is done via computer transactions between trusted organizations who allow each other to post credit or debit transactions, usually through a third party clearing house company to ensure that the transaction is legitimate and that funds are available in the card holder's database account to allow the transaction to successfully proceed.

Therefore, what we think of as "money" anymore is nothing more than database manipulation of transactions between trusting institutions over network connectivity.

Encryption Alone Cannot Protect Information

A major problem with such transactions is that there are long-standing, misguided beliefs that technologies such as encryption will solve the security aspects of "trust" between the organizations which allow the transactions to happen. The reality is that an encrypted value in a database cannot be changed. Therefore, encryption is used as a secure method to get the information to the database, not to actually secure the manipulation of the value.

More specifically, we might use encryption from the source location to the destination location to "hide" personal and private data from being viewed on the networking components as the packets traverse the Internet. Ultimately, however, when the information arrives at the destination database server, it must be decrypted and then the database manipulated to change (credit or debit) the user's financial account information based on requests that are encoded as part of the transaction. This encoded entry cannot be encrypted or the values could not be changed. This means that, ultimately, the identity level of "trust" of the originating requestor of the transaction is a problem in financial transactions.

For example in the physical world, how does the bank database at your financial institution really know that it is you, in person, presenting a credit card with a magnetic strip and running it through the card reader at the grocery store? It "believes" that the information presented to it via the transaction request is authentic, based upon the fact that a physical card is required at the originating point and the general belief that you, as a person, are the only individual who has your card in your possession and would be using that card.

Card companies go to great lengths to monitor card request activities to detect fraudulent actions. For instance, if your card is being used in one geography and then, suddenly, is used in a human-interactive way in a radically different physical place, fraud management facilities at the member financial institutions will detect this as abnormal behavior and potentially stop the card transaction, initiate a call to the card holder or a variety of other actions. All of this is well and good, but it is based on a singular premise that the authentication method used in most credit cards, even at the physical card level, can be "spoofed" or faked and the card companies must take additional actions to monitor transactions to ensure they are legitimate.

Identify Management is a Key Component To Avoid Outages

The real problems of identity management are actually much broader than those posed via individual identity theft or via credit card fraud. In fact, debilitating cyber attacks are launched daily on the Internet and private networks via a type of attack called a distributed denial of service (DDoS) attack.

In this type of attack, an attacker will use anywhere from one to several thousand "slave" (or "zombie") PCs to send packets with forged source addresses (a technique called "spoofing") to a destination network address for the purposes of clogging up the network connection to the address so that it cannot be used by legitimate transactions. This type of attack is successful largely because a source address on most networks is automatically assigned to a system "joining" the network without properly establishing the identity of the computer when it joins the network. Specifically, does a particular system requesting an address from a network provider actually "belong" to the organization or is it authorized to "join" the network, be assigned an address and then use the network?

The reality is that the Internet and other TCP/IP networks continue to use a protocol suite that is over 30 years old and does not contain any security or identity management capabilities. If it did, the ability to "spoof" an address would disappear and such attacks would not be possible. DDoS attacks are commonplace, debilitating and cause a wide variety of network outages on a daily basis on thousands of networks worldwide. Worse, as society becomes more dependent on e-commerce methods and techniques, the effect of a DDoS attack on businesses becomes more debilitating to the company's bottom line. As an example, consider that power grid networks are migrating from legacy protocol suites such as DECnet and OSI to TCP/IP. As this migration happens, more and more previously private networks are eventually connected to public networks such as Internet. Also, the protocols being deployed do not have base security capabilities in them to differentiate which systems are allowed to be on a specific network and which ones are not. As a power grid network is migrated to TCP/IP, it becomes increasingly vulnerable to DDoS attacks as systems on the network do not have to provide proof-positive that they belong to the network and

can send packets to a destination via spoofing attacks. In the case of a power grid, this type of attack will not only debilitate the network, it will cause grid management systems to not be able to respond to each other in a timely fashion, which will ultimately lead to system disconnections from the grid network. This type of action means that power grids will not be able to interconnect and share load information and will cause a grid to become unstable and force a computer shutdown. This type of situation will cause a mirror of what happened in August, 2003, when the power grid in the Northeast U.S. caused a computer-controlled shutdown of connected plants.

Without basic identity management of devices that "join" a network, it is impossible to stop DDoS attacks and their ilk. It also means that simple methods to kill networks will continue to exist until management of system identities is provisioned as part of the basic protocol methodology when a system joins a network and is assigned an address to communicate with other systems on the network.

Identiy Mangement is a Key Component for All Infrastructure

Simplistic identity schemes, such as human-readable passwords, are commonly used for network switches and routers, the core components of modern communications networks which drive all manner of connectivity from telephones to cable television. Many times, passwords are shared and easily trapped by hacker programs, which grab passwords off networks or are easily guessed due to the simplistic nature in which the passwords are created and assigned to systems, devices and applications. The use of traditional passwords for infrastructure (and, frankly, any other system or application) is akin to using a screen door on a submarine for access to/from the vessel (on the positive side, the screen door probably helps keep the fish out when submerged).

In addition, very often, database-to-database "glue" programs are initialized and set-up with a single user ID and password to allow databases to interoperate and exchange information. This is a very normal occurrence where front-end, web-based engines access legacy mainframe databases to move data between the front end user method and the backend mainframe database. These passwords are the human-readable password types and not a cryptographically sound methodology. The destination back-end database system will often list the single user ID and password of the requesting user for all database transactions, no matter how critical or secure they must be, from the front-end database engine. The result is that if anyone gets access to the front end and can bypass any control methods between the databases (and his happens relatively frequently), the default access ID and password are easily discerned and the attacker can access the backend database and data with impunity.

Conclusions and Possible Solutions

In all situations I have discussed, the basic problem of identity management of devices, applications and individuals becomes a central problem in providing a safe transaction or computing environment. Identity management of the future cannot be the simplistic password methods of the past – it will need to incorporate advanced concepts such as biometrics and cryptographically sound methods to ensure the identity of a device, application or individual is permitted to access data elements in databases and other information repositories.

So, what kind of potential solutions are available to solve these identity issues?

1. Network and application protocols need a "heavy lift" R&D and engineering effort put behind them to include security controls and methods for identity management. Inclusion of identity management techniques and methods needs to be carefully considered, tested and implemented to be successful over the long term or the problems being currently experienced will pale in comparison to what will happen longer term as U.S. society becomes more entrenched in technical methods to interoperate and exchange critical financial and personal data over networks.

2. Strong, effective individualized identity methods for U.S. citizens needs to be established in a cryptographically sound manner. Simple picture IDs issued by state governments will not suffice with interstate commerce electronic transactions; advanced concepts utilizing biometrics, cryptographically secure "smart cards" and other strong authentication methods that are securely implemented need to be completed at a national level to ensure that individuals presenting identification credentials are who they claim to be and cannot be spoofed.

3. Authentication implementation and audit rules/processes need to be established for critical infrastructures such as power networks, water processing networks, food supply, telecom supply, emergency services and other related types of network infrastructures which are becoming totally dependent on technologies to be effective.

4. Multiple methods of authentication standards need to be created and established to ensure that one authentication method, if compromised, does not cause the "house of cards" scenario and take down all other authentication methods in the process. While more technically difficult to implement, it supplies one of the base rules of computer security – defense in depth – and allows for the eventuality of any specific security component being breached by having multiple authentication methods, properly compartmented from each other.

5. Incentives need to be provided to various sectors to rapidly implement advanced authentication and identity management methods. These may

vary in composition, but might include items such as reduced legal liability if a company implements strong authentication and identity management processed and technologies on critical infrastructures or areas where privacy is paramount.

6. The U.S. government needs to lead from the front. For example, U.S. government contractual and licensing agreements need to include strong authentication and identity methods as a requirement for the purchase of products and services which provision network, database or applications connectivity. Also, there needs to be a requirement that interconnection to private sector or other public organizations (such as municipalities and state governments) possess the same if not superior authentication and identity management schemes before such connectivity is allowed.

7. There needs to be an effort to quickly compel the government and public companies to migrate away from traditional (and very weak, security-wise) human-readable and guessable passwords and access methods. The time for such controls is antiquated and are grossly insecure.

8. We need to take an international approach. For example , we could couple U.S. trade agreements with international partners to include strong authentication and identity management for all electronic transactions of any type. While this will take time, oddly enough other countries (such as Malaysia) are ahead of the U.S. in the areas of national identity management and in their government use of strong authentication methods. The U.S. cannot be left behind on this important and mission critical issue.

9. We need to migrate traditional U.S. government functionality dependency on commonly accessible information, such as Social Security numbers, and migrate to strong authentication and multi-level identity management schemes to protect citizen privacy and confidentiality of information.

10. Any legislative or regulatory efforts in the area of identity management need to be on a larger scale than just the protection of a password, an individual's private information or a financial transaction. Identity management is a key component of a multi-level security strategy to properly protect critical infrastructures at many different control points. Identity of devices, applications, individuals and the mixing/matching of all comprise a wide range of identity management challenges that must be solved to ensure that the U.S. economy stays safe and secure.

Thank you, Mr. Chairman, for the opportunity to testify today. I will now be happy to take any questions.

Mr. PUTNAM. Our next witness is Bill Conner. Mr. Conner is among the most experienced security and infrastructure executives worldwide, with a career that spans more than 20 years across numerous high-tech industries. Mr. Conner joined Entrust as its president and CEO in April 2001. In 2003, Mr. Conner received the corporate CEO award as part of the annual Tech Titans Award program. Most recently he has been a leader in the effort to elevate information security to a corporate governance issue and to fashion a public-private partnership to protect America's critical infrastructure.

Welcome to the subcommittee, Mr. Conner. You are recognized for 5 minutes.

Mr. CONNER. Thank you, Mr. Chairman. Good afternoon. Chairman Putnam, Representative Clay, and members of the subcommittee. Thank you for the opportunity to provide testimony on this important subject.

My name is Bill Conner. I am chairman, president, and CEO of Entrust. In my testimony today I will address the threat of identity theft and phishing. I will also examine what Congress can do about it.

I want to be very clear in my message: Identity theft and phishing threaten not only to undermine the trust in business and the Internet, but also to disrupt our national economy. We need to protect all Internet users, not just the upper tier. Identity theft and phishing do not discriminate between the haves and have-nots, and corporate programs aimed at protecting only the most valued customers won't solved the problem. These are not isolated threats, but part of a broader cybersecurity challenge.

I would like to first address why identity theft and phishing are serious problems. Just as the Internet has supercharged commercial transactions, it has also supercharged cybercrime. When the Internet was used mainly to communicate and access information, the lack of security didn't much matter. Now that it is used for on-line transactions and critical information, the absence of security is truly a big problem. It is as if consumers and businesses that rely on the Internet have wandered into a dangerous neighborhood of cheats, pickpockets and thieves and don't even know it. The fact that 9 percent of U.S. on-line consumers have experienced identity theft and that phishing attacks are now growing at 50 percent per month show that the little yellow locks on your desktop that are supposed to maintain law and order on the Internet are inadequate.

The obvious question is why? Why has the market been so slow to respond? As a result of my role at Entrust and my experience as cochair of two major task forces on information security, I have become convinced that the only way for enterprises to address cybersecurity is to make it an executive management priority with board oversight. This is not the case today.

There are several reasons for the lack of progress. One, companies don't know what to do. Many companies don't understand the scope or the threat and how to respond. As a result, they pretend the problem doesn't exist, and, if it does, it won't hurt them.

Second, it is not a corporate priority. Even if they understand it, many firms refuse to make it an executive priority. They continue

to treat cybersecurity as a technical issue and one that can be delegated and relegated to the CIO.

Government regulations are unclear. A raft of legislation has been passed in recent years including GLB, HIPAA, California's Senate bill 1386, and most recently section 404 Sarbanes-Oxley. Until there is better understanding of what it takes to comply and the penalties for the failure to do so, progress will be slow.

And, fourth, technology vendors aren't doing enough. Vendors share in this blame. We have been criticized for overhyping solutions, failing to correct and connect products to business needs, ignoring ways to measure the return on investment, and producing poor-quality products that constantly require patching.

That is why I urge you to consider the road to information security lies through corporate governance. If the government and private sector are to secure their information assets, they must make cybersecurity an integral part of internal control and policies. Like quality, cybersecurity is a journey of continuous improvement, not a one-time event. The No. 1 priority for Congress should be to create a bright light between acceptable and unacceptable behavior. As long as the line is fuzzy, the market will be caught in the cybersecurity paradox. Everyone knows there is a problem, but in the absence of clear solutions or penalties, they are waiting for someone else to take the lead.

I would offer the following recommendations for your consideration: One, Congress should demand that Federal agencies purchase and deploy cybersecurity technologies. Mr. Chairman, as part of your oversight of FISMA, I would urge you to initiate a dialog about how to drive deployment of security technology that Federal agents have purchased but left sitting on the shelf.

Two, Congress should stipulate that cybersecurity measures are an explicit part of Sarbanes-Oxley section 404. By stating that section 404 Sarbanes-Oxley applies to cybersecurity controls, Congress could encourage publicly traded companies like mine to make information security governance a corporate policy and priority.

Third, the Federal Government should lead by example. Congress should discourage Federal agencies from purchasing products from companies with inadequate cybersecurity, as well as create incentives for those that implement formations of cybersecurity governance programs. An example of such a program can be found in the report, "Information Security Governance: A Call to Action," that was released by the National Cybersecurity Partnership Task Force on Corporate Governance in April of this year.

Mr. Chairman, the cybersecurity threat is real and holds potential to incapacitate the Internet and our economy. The private sector has been much too slow to respond to this challenge. I would urge you and your colleagues in Congress to spur a rapid and constructive market response.

Mr. Chairman, I would personally like to thank you for your leadership and your staff's in taking the lead and the initiative here in this area.

Mr. PUTNAM. Thank you very much, Mr. Conner.

[The prepared statement of Mr. Conner follows:]

Statement of Bill Conner

Chairman, President and CEO

Entrust, Inc.

Before

The House Government Reform Committee

Subcommittee on Technology, Information Policy,

Intergovernmental Relations and the Census

"Identity Theft: The Causes, Costs, Consequences, and Potential Solutions"

September 22, 2004

Good Morning. Chairman Putnam and Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject. My name is Bill Conner, and I am Chairman, President and CEO of Entrust, Inc. In my testimony today, I will address the threat of identify theft and phishing and examine what Congress can do about it.

I want to be very clear in my message. Identity theft and phishing are serious problems that threaten not only to undermine trust in business and the Internet, but also to disrupt our national economy. They are not isolated issues that can be tackled by themselves, but part of the broader cyber security challenge facing the networked economy. Although some companies have recognized the importance of cyber security to their business, most are struggling with it. It is incumbent on this Subcommittee to galvanize government and industry to implement strong cyber security programs.

Entrust is a world leader in securing digital identities and information. Over 1,200 enterprises and government agencies in more than 50 countries use our security software solutions, so we have a good perspective on today's cyber security reality. As a company, we are leading the evolution from defensive-oriented security technology approaches to a more proactive business security strategy that not only protects information assets, but also enables business needs. This strategy involves creating a more robust, manageable business security environment through the use of technologies such as encryption, digital signatures, authentication and authorization. Our mission is to

work with customers to put in place the technologies, policies and procedures necessary to protect digital identities and information.

Over the past two years, I have co-chaired two major cyber security task forces: 1) the Business Software Alliance Task Force on Information Security Governance, and 2) the National Cyber Security Partnership Task Force on Corporate Governance. Through this work and my professional experience at Entrust, I have become convinced that the only way for enterprises to address cyber security is to elevate the issue to executive management with board oversight within an information security governance framework. Although Congress has passed several cyber security bills in recent years, each addresses only one facet of the problem. Because cyber security is a constantly moving target, I do not believe that this piecemeal approach will be successful. Only by treating cyber security as a governance issue and adhering to a specific information security governance framework for employees at all levels, can organizations truly make sustained progress.

I. What are identity theft and phishing, and why are they such serious problems?

Just as the Internet has supercharged commercial transactions, so has it heightened the potential for cyber crime. Identity theft is an especially pernicious form of cyber crime, and phishing is an especially potent form of identity theft. Identity theft consists of stealing a corporation's or individual's identity and using it for illegal purposes. Phishing consists of using "spoofed" e-mails and phony websites to fool recipients into divulging sensitive personal financial information, such as credit card numbers, social security numbers and passwords. By masquerading as reputable companies, phishers have

already lured up to 5% of recipients to respond to their false representations, and this crime is still in its infancy.

Over the past decade, consumers, enterprises and governments have become increasingly dependant on the Internet. What began as an easy way to communicate and access information has evolved into a means of conducting on-line transactions, integrating strategic relationships and managing customer accounts. Unfortunately, as critical applications and sensitive information have moved onto the Internet, security has not kept pace. As a result, many consumers and businesses are walking in a dangerous neighborhood and don't even know it. A few statistics demonstrate the seriousness of the problem.

- The US Federal Trade Commission has highlighted identity theft as the fastest growing white collar crime in America with annual losses of $9 billion in 2003. Computer Economics, a technology consulting firm, estimates that losses will grow to over $16 billion by the end of 2004.
- According to Forrester Research, 9% of US online consumers (an estimated 6 million households) have experienced identity theft.
- Industry associations report that phishing attacks are now growing at over 50% per month.

Despite these alarming statistics, many consumers still don't understand the problem, and business has been slow to address it. Part of the problem is that phishing attacks are becoming more and more sophisticated. Today's scams are like counterfeit money – they

are so carefully rendered that many consumers believe they are legitimate and therefore provide sensitive information freely. The biggest barrier to progress, however, is the business mindset about cyber security. Despite the fact that businesses face serious financial risks from identity theft and phishing, most companies take inadequate cyber security precautions.

II. What is the Market Response?

The market response falls into three categories: 1) Do nothing; 2) Take limited precautions; and 3) Attack the problem internally and externally. Each of these is examined below.

Do Nothing

Too many companies continue to ignore the problem, pretending that it doesn't exist, or if it does, that it won't have an impact on them. According to *The State of Information Security, 2004* (a worldwide survey of more than 8,100 IT security professionals in 62 countries compiled by CIO Magazine and PricewaterhouseCoopers), 8% of organizations admit that they have no formal security policy, and the real number is probably higher. There are many reasons for this failure to take action.

1. *They don't know what to do.* Despite the fact that identity theft and cyber crime are growing exponentially, many companies are still unaware of them. For example, in our discussions with a Fortune 500 health care provider during the past few months, we were surprised to learn that their CIO had never heard of

phishing. Even when companies are aware of the problem, they often resist taking action because of concern about inconveniencing their customers. For example, a major bank realized that it did not have adequate cyber security protections to securely authenticate its sensitive communications, but was unwilling to accept any solution that required more than a few milliseconds response time for authentication during fail-over. Since no security products met this standard, the bank was unwilling to implement a solution. In the absence of a clear course of action, many firms are waiting for others to take the lead. This behavior has created a "chicken-and-egg" conundrum -- everyone knows there is a problem, but they won't act aggressively until others do.

2. *It's not a corporate priority.* Many firms are unwilling to elevate identity theft (and the need for a cyber security program that it implies) to the attention of senior management. *The State of Information Security*, 2004 reports that 20% of IT security professionals cite limited support from executives as a barrier to good security. This statistic indicates that many organizations continue to treat cyber security primarily as a technical issue that can be delegated to the CIO, not as a governance issue that requires the attention of boards, CEOs, and business unit heads. This failure to make cyber security a corporate governance priority often leads to a failure to implement solutions. All too often, even when organizations do buy technology to secure their operations, they never fully deploy it because there is no plan or connection back to their business needs. Federal agencies are only too familiar with this problem.

3. *Government regulations are unclear.* A raft of legislation has been passed in recent years that addresses cyber security issues, including the Financial Modernization Act (Gramm-Leach-Bliley), the Health Insurance Portability and Accountability Act (HIPAA) and California Senate Bill 1386. Section 404 of the Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley), with its focus on appropriate "internal controls" for financial information, also raises questions about cyber security. Each of these laws addresses different aspects of the problem, and each is the subject of extensive debate. Until there is better understanding of what it takes to comply with these laws and the penalties for failure to do so, progress will be slow.

4. *Technology vendors aren't doing enough.* Many enterprises and consumers criticize technology vendors for producing poor quality products with security holes that require constant patching. Others blame vendors for over-hyping their solutions, failing to connect them to business needs, and ignoring ways to measure return on investment. Still others fault the complexity of the technology itself. Vendors are working to respond to these criticisms since they understand that cyber security technology must be more closely integrated with applications and easier to deploy and use if it is to be widely embraced.

Take Limited Precautions.

Most companies fall into this category. They know that they must do something to satisfy customer expectations, but are worried about any inconvenience that may result. Similarly, they know they must meet government regulations, but are confounded by the vagaries of current legislation. Even when they do take action, they are reluctant to speak openly about it out of concern that doing so will increase their liability and make them a target for hackers. According to *The State of Information Security, 2004*, over half of IT security professionals are not reporting breaches at all. These organizations tend to do lots of studies, pilots and tests. They may deploy some technology around the margins that is easy to implement, but never commit to implementing a robust cyber security solution. Keeping out of trouble with management and doing just enough to satisfy regulators seems to be the goal, not implementing solutions that are based on careful risk analysis and that address business needs.

Attack the problem internally and externally.

Very few companies have made cyber security a corporate governance priority by linking it to their business needs, implementing strong internal controls, and focusing public attention on the issue. Those that have tend to be banks, on-line retailers, companies in the cyber security industry or organizations that have experienced significant breaches. These companies do not view cyber security as an isolated problem that can be addressed once and forgotten. Nor do they view it as a consumer problem. Instead, they embrace it as a core business issue that requires continuous vigilance and sustained progress, much like quality assurance. Even these organizations, however, still have a long way to go. I

can speak from personal experience here, because even though Entrust has had an information security governance framework in place for two years, we still have a lot of work ahead of us. Cyber security is a journey, not a one-time event, and policies must be systematically reviewed, measured and refined. Even when companies do implement cyber security programs, they often fail to follow up with the proper oversight. According to *The State of Cyber Security, 2004* only a little over one-third of organizations with cyber security policies have measured and reviewed them.

I believe that the road to information security lies through corporate governance. If the government and the private sector are to make significant progress securing their information assets, executive management must make information security an integral part of core business operations. There is no better way to accomplish this goal than to highlight it as part of the internal controls and policies that constitute corporate governance and create a framework that defines tasks for employees at all levels of an organization.

There is a lot of consumer data that supports the wisdom of an aggressive cyber security program.

- According to a survey that Symantec conducted with InSightExpress, over 40% of consumers are very concerned about online fraud, and the majority of respondents have changed the way they use the Internet because of their concerns. About 32% of them won't use the Internet for online banking, and almost 15% say they don't trust the Internet.

- Worry about identity theft is even more acute among online users. According to Forrester Research, 61% of online consumers are extremely or very concerned about it.
- According to research commissioned by Entrust, 80% of Internet users are worried about someone stealing their on-line identity and using it to access their on-line bank accounts. Importantly, 72% of them would use online banking if online identity security was improved. And 90% of existing online bank users would take advantage of additional, higher value services if their online identities were better protected.
- One-in-five user-name/passwords is breached. According to Entrust's research, most Internet users would be willing to change their habits to better protect their identity. For example, 78% would be willing to use a second factor of authentication when accessing their bank accounts to improve the security of their identity.

IV. What are the lessons?

We can draw several lessons from the threat that identity theft and phishing pose. These lessons, in turn, point the way to constructive Congressional action.

- Identity theft and phishing are extremely serious problems that, left unchecked, have the potential to undermine many e-commerce and e-government applications that depend on trust in the Internet.
- They are not isolated problems, but part of the broader cyber security challenge.

- Current laws tend to treat cyber security as a secondary issue. As a result, they cite requirements that are vague and don't do enough to advance understanding of the costs and benefits that are necessary for industry to orchestrate an effective response.
- The private sector has not taken action sufficient to address the problem and is still reluctant to talk openly about it.
- Companies must build better products. Entrust and others are doing just that, and soon will have new solutions that are inexpensive and suited to the mass market.
- Technical solutions alone are not enough. They must be coupled with information security governance programs that make cyber security an integral part of the on-line experience.
- Education is important, but by itself is insufficient since it assumes that the problem rests with consumers, not with business.

V. What is the role of Congress?

Congress has a vital role to play in addressing the related threats of identity theft and phishing. Its number one priority should be to create a bright line between acceptable and unacceptable behavior. As long as this line remains fuzzy, the market will be caught in a cyber security paradox – everyone knows that it is a serious problem, but in the absence of clear solutions or penalties they are waiting for someone else to take the lead.

As mentioned earlier, it is difficult to address phishing and identity theft in isolation since they are part of an overall cyber security problem. Recognizing that fact, I would like to offer the following recommendations for consideration by the Subcommittee:

1. **Congress should demand that Federal agencies purchase *and deploy* cyber security technologies.** Although Federal agencies purchase a lot of technology to secure their information assets, they often fail to deploy it fully. This issue is especially relevant for this Subcommittee since you have jurisdiction over technology and information policy for the Federal government. Mr. Chairman, as part of your oversight of the Federal Information Security Management Act (FISMA), I would urge you to initiate a dialogue about how to drive implementation of cyber security technologies that Federal agencies have purchased but not fully implemented. As part of this discussion, you should examine how both carrots and sticks can accelerate deployment.

2. **Congress should stipulate that cyber security measures are an explicit part of Section 404 of the Sarbanes-Oxley bill.** Section 404 of Sarbanes-Oxley requires senior management of publicly traded companies to establish and maintain adequate internal controls for financial reporting and to assess the effectiveness of these controls annually. It does not mention cyber security, but it is hard to escape the conclusion that publicly traded companies cannot protect their financial information (most of which is kept in digital form) without employing some sort of cyber security. This lack of specificity adds to the confusion

surrounding private sector efforts to secure digital identities and information. By stipulating that Section 404 of Sarbanes Oxley applies to cyber security controls, Congress could encourage publicly traded companies to make information security to a corporate governance priority.

3. **Congress should drive implementation of the Homeland Security Presidential Directive HSPD-12.** This Directive is designed to provide Federal employees with digital credentials that provide strong authentication and can be used to secure identities, information and transactions. The key to effective deployment is to integrate these credentials with new and existing applications. Unless this integration is done without significantly revising existing applications, these credentials will just sit on a shelf. Just as this Subcommittee has effectively used FISMA to drive Federal implementation of cyber security programs, so should it use HSPD-12 to grade and discipline the roll-out of digital credentials. Doing so would accelerate implementation, provide for consistent delivery and spur immediate usage. The capability to issue these digital credentials already exists in many Federal agencies, and by linking architecture with applications Congress could help spur the Federal E-authentication program.

4. **The Federal government should lead by example.** Congress should discourage Federal agencies from purchasing products from companies with inadequate cyber security programs or a record for poor quality. Congress should also create incentives for companies that institute robust information security governance

programs. An example of such a program can be found in the report, Information Security Governance: A Call to Action, that was release by the National Cyber Security Partnership Task Force on Corporate Governance in April 2004. To be effective these information security governance programs should be regularly reviewed, measured and updated.

The identity theft and phishing epidemic shows that the cyber security threat is real and has the potential to incapacitate the Internet. The private sector has been slow to respond to the problem, and Congress should consider ways to spur a more constructive market response.

Mr. PUTNAM. Our next witness is Jody Westby. Ms. Westby recently joined PricewaterhouseCoopers as a managing director. Prior to joining PricewaterhouseCoopers, Ms. Westby held several positions in the IT field including serving as president of her own company, launching an IT solutions company for the CIA, and managing the domestic policy department for the U.S. Chamber of Commerce. She is the chair of the American Bar Association's Privacy and Computer Crime Committee, and was Chair, coauthor and editor of its International Guides to Cybersecurity, to Privacy, and to Combating Cybercrime.

Welcome to the subcommittee. You are recognized for 5 minutes.

Ms. WESTBY. Thank you, Mr. Chairman, Mr. Clay. I appreciate the opportunity to be here this afternoon. I would like to clarify at the outset that my remarks, my testimony, is in my individual capacity and is based on my own background and experience. It does not necessarily reflect the views of the American Bar Association or PricewaterhouseCoopers.

I applaud your attention to this critical issue. The security breaches that allow access, unauthorized access, to personally identifiable information go beyond unauthorized credit card charges, although that is in and of itself a grave issue. This data also feeds terrorist organizations, organized crime, and other bad actors that can use this information to exploit us for their own good, and to launch asymmetrical attacks against us.

Because 85 percent of our information infrastructure in this country is owned by the private sector, the only way we can control these risks and protect our national and economic security is to protect the critical infrastructure of the companies. Herein lies the problem. Technical solutions alone will not secure our networks.

Time and again over the past decade, hardware and software has held hope that we could turn the tide. But the truth is the bad guys are winning. The root of the problem is that there is a lack of oversight and governance of enterprise security programs by senior management and boards. Quite simply, we must change the paradigm for information security.

Part of the problem is perception. Most people think of information security as a technical issue. It is really a multifaceted issue that requires a multidisciplinary approach. It is multifaceted because it involves privacy and security and cybercrime. It is multidisciplinary because it requires you to dovetail the legal, operational, managerial, and technical considerations of all three of those issues piled in with the business plan that sets the architecture of a company. It is a complicated process.

I believe the main reason privacy has taken off is because people perceived privacy—CEOs and boards—readily at the beginning as a policy issue. They readily appointed a chief privacy officer, they put out policy statements, and privacy was accepted as a corporate governance issue.

Security, on the other hand, is still perceived as a geek issue. CEO and boards are afraid of becoming geeks. The primary reason senior management and boards don't want to take on these issues is because they don't know how to approach it from a governance perspective. They think they have technical people to take care of

the computers, so why should they worry about it; they hired them; that is their responsibility.

That is the wrong conclusion. Information and communication technology comprises one of the largest line items in corporate budgets. Officers and directors have a responsibility to exercise oversight over this equipment for the very reason that the viability and profitability of their corporation is dependent on it. Also, 80 percent of corporate assets today are digital. It is clear that directors and officers have a fiduciary duty of care to protect business assets. There also remains a high incidence of insider attacks, yet these are the very people who are under the direct control of boards and senior management. Companies also have a patchwork of laws and regulations they must comply with in the area of privacy and security, and compliance has always been viewed as a governance issue.

Studies have shown that cyberattacks can impact market share and share price, two key areas of responsibility for officers and directors. A Delaware derivative shareholder case, Caremark, in 1996 was brought to the attention of the information security world because it emphasized that boards have to ensure that their corporate information reporting systems are, in concept and design, adequate.

And the last reason why officers and directors need to pay attention to this is because cyberattacks are so common today. They are in the daily news. Leaving networks unsecured is the equivalent of leaving the R&D lab door unlocked.

There are other consequences also that require consideration, one which was brought up by my colleague today about the inability to track and trace cyber incidents. Cyber incidents frequently pass through many countries, and we involve international cooperation of law enforcement, we have dual criminality issues, we have extradition issues. But terrorists and organized crime are exploiting this inability to track and trace cyber incidents, and they are using that as a way then to obtain this information and use it for trafficking of drugs, money laundering, and purchasing weapons and supplies. Corporations and data banks are their soft targets, and this puts us all at risk.

Quite simply, corporations have to begin viewing security as an enterprise issue that is also a governance issue. Prevention of attacks is the best problem, and Congress can help them do that by providing tax credits to corporations that implement enterprise security programs. Such credits could encompass risk assessments, implementing best practices and standards, establishing internal controls, integrating security, and of capital planning and training.

Another initiative could provide some funding grants to help advance models for effectively measuring return on investment for information security programs, and other tools that would help boards and senior management through the decisionmaking progress.

Last, I want to stress that this is not just a U.S. problem, it is a global problem. The global security of the Internet has never been more important. We are close to a saturation point among the English-speaking populations in the world. Connectivity in the fu-

ture will be in Asia-Pacific, Europe, and Latin America, in that order.

In a globally connected network, we are only as secure as our neighbors, and we must help them if we are to help ourselves. We have to help them draft privacy, security, and cybercrime laws that are consistent with FISMA and the global framework; to help them understand the nexus between privacy, security, and cybercrime, and how to build enterprise security programs using the best practices and standards; and, as our earlier panel said, to train law enforcement and judges and prosecutors.

The good news is this all repeatable. In the past several years I have done a lot of work in developing countries. Road shows with consistent materials trotted around the globe would be very effective.

I am sorry, Mr. Bordes, do you have the three books that I brought up here? Could you please share those with Congressmen Clay and Putnam?

These books are available. The American Bar Association's Privacy and Computer Crime has put its money where its mouth is. These books are free to people in developing countries. That is 180 countries around the world, they are free to them, and they set out all the issues of privacy, security, and cybercrime, and how to develop an enterprise security program. Our books would significantly improve our own security and advance world peace if we were able to get them into audiences as workshops and textbook materials.

Thank you very much for your interest, and I await your questions.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Ms. Westby follows:]

TESTIMONY OF

Jody R. Westby, Esq.
Managing Director, PricewaterhouseCoopers LLP

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

September 22, 2004

INFORMATION SECURITY: RESPONSIBILITIES OF BOARDS OF DIRECTORS AND SENIOR MANAGEMENT

Introduction

Good afternoon, Mr. Chairman and Members of the Subcommittee. My name is Jody Westby. I am a Managing Director of PricewaterhouseCoopers LLP, and I currently chair the American Bar Association's Privacy & Computer Crime Committee, Section of Science & Technology Law. I would like to state at the outset, for clarification of the Subcommittee, that I am here today testifying in my individual capacity and that my testimony is based on my own background and experience, and does not necessarily reflect the position of the American Bar Association or PricewaterhouseCoopers.

It is an honor to participate in this important discussion on the ramifications of identity theft. Thank you for including me among these distinguished panelists. I have been working in the field of information technology (IT) security since 1996, with an emphasis upon the role of boards of directors and senior executives in protecting their corporate information infrastructure since 1998. The perspective I bring to the Subcommittee today is based on more than twenty years of technical, legal, policy, and business experience, enabling me to bring a multidisciplinary perspective to the many issues facing businesses and governments in the areas of information security, IT business risk management, outsourcing/offshoring risks, cybercrime, and Homeland Security, including cyberterrorism and infowar. I am a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security and serve on the board of the National Conference of Lawyers and Scientists. In my professional capacity, I regularly consult with governments, private sector executives, and operational personnel on the development of enterprise security programs that dovetail the technical, legal, operational, and managerial considerations.

Today, our national security, economic security, and public safety are intertwined due to the risks flowing from a global network connecting over 730 million users in nearly 200 countries. Identity theft is but one vulnerability. Security breaches that result in unauthorized access to personally identifiable information provide the data needed for identify theft. In addition, these breaches can feed organized crime, terrorist organizations, and other bad actors information that enables them to exploit others for their benefit or launch asymmetric attacks that jeopardize public safety and our national and economic security. Our ability to control these risks is largely

dependent upon the security of private sector networks. My testimony will focus on the root-cause of electronic identity theft: the lack of enterprise security safeguards that are governed by boards of directors and senior management, including the implementation of best practices and standards and regular risk assessments.

Although the financial sector is ahead of other industries in this area, overall, there remains a disturbing lack of understanding at the officer and director levels regarding their oversight and governance responsibilities for the security of corporate data, applications, and networks. These responsibilities include:

- Regularly assessing information technology (IT) risks to corporate operations and managing identified threats and vulnerabilities;
- Establishing corporate policies governing IT usage, cyber security, and employee conduct;
- Incorporating cyber security best practices and standards into business operations;
- Ensuring sufficient funding is allocated to develop and maintain an enterprise security program with adequate internal controls;
- Implementing the security program through training and measuring compliance through meaningful metrics; and
- Conducting regular reviews and audits of the security program.

Unfortunately, the good work of many to move corporate America in this direction is being undercut by the notion that risk assessments – the critical input necessary for any enterprise security program – can establish knowledge of system vulnerabilities and weaknesses that later could be used against a corporation in the event of a cyber attack or security breach that caused harm to others or resulted in economic losses. Indeed, that could be true if serious weaknesses were identified and no corrective measures were taken. This, however, is no different than the consequences of ignoring structural or mechanical weaknesses after a review process.

My testimony rebuts this notion by asserting that corporations – including their officers and directors – actually *increase* their risk to liability if they fail to (1) conduct assessments, (2) meet security and privacy compliance requirements and legal obligations, and (3) develop and implement an enterprise security program that mitigates identified risks and adheres to best practices and standards. Today, cyber incidents are in the daily news and their general impact upon corporations operations is well known. Moreover, a plethora of standards, best practices, and guidance exists to assist companies of all sizes in protecting their systems. In addition, a sizeable percentage of private sector companies are now subject to numerous security compliance responsibilities. This heightened level of awareness, combined with new legal security requirements and industry acceptance of security standards and best practices, make risk assessments a corporate responsibility to be accepted, not ignored.

This testimony steps through director and officer responsibilities for cyber security, including the major compliance requirements; it discusses the current situation and threats; and suggests possible steps toward advancing cyber security at the corporate level and around the globe.

The starting point is to determine the *responsibility* that boards and officers have to protect their digital assets, which includes information, applications, and networks. In the U.S., this responsibility flows from two sources:

1. Case law surrounding the fiduciary duty of care directors and officers owe their shareholders and the protections afforded by the "Business Judgment Rule;" and

2. Compliance with statutes, regulations, Executive Orders and Presidential Directives, administrative consent decrees, contractual agreements, and public expectations.

From an international perspective, the Council of Europe Convention on Cybercrime[1] (CoE Convention) and the European Union's (EU) Council Framework Decision on attacks against information systems[2] both specify administrative, civil, and criminal penalties for cybercrimes that were made possible due to the lack of supervision or control by someone in a senior management position, such as an officer or director.[3]

Duty of Care and Business Judgment Rule[4]

Director and officer governance of corporate digital security is embedded within the fiduciary duty of care owed to company shareholders to:

- Govern the operations of the company and protect its critical assets;
- Protect the company's market share and stock price;
- Govern the conduct of employees;
- Protect the reputation of the company; and
- Ensure compliance requirements are met.

---

[1] Council of Europe *Convention on Cybercrime* – Budapest, 23.XI.2001 (ETS No. 185) (2002), http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm, Council of Europe *Convention on Cybercrime Explanatory Report*, Nov. 8, 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (hereinafter referred to as "CoE Convention").

[2] *Proposal for a Council Framework Decision on attacks against information systems*, Commission of the European Communities, Article 9, Apr. 19, 2002, COM(2002) 173 final, 2002/0086 (CNS), http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf (hereinafter referred to as EU Council Framework Decision").

[3] CoE Convention, Article 12; EU Council Framework Decision, Article 9. The U.S. is a signatory of the CoE Convention and on November 17, 2003, President Bush sent the Convention to the U.S. Senate for ratification, but action has not been taken. *See* George W. Bush, "Message to the Senate of the United States," The White House, Nov. 17, 2003, http://www.whitehouse.gov/news/releases/2003/11/print/20031117-11.html.

[4] Significant portions of the text in this section are taken from the following two sources, of which I own the copyright to the text: Jody R. Westby, ed., *International Guide to Cyber Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2004 at 191-93 (hereinafter "Westby - Cyber Security"); *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report & Recommendations, World Federation of Scientists, Permanent Monitoring Panel on Information Security, Nov. 19, 2003, World Summit on the Information Society Document WSIS-03/GENEVA/CONTR/6-E, http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (hereinafter "Toward a Universal Order of Cyberspace").

Duty of Care

Directors and officers are responsible for governing the operations of a company. This includes the protection of critical assets. Since an estimated 80 percent of corporate assets today are digital,[5] it logically follows that the oversight of information security falls within this duty. Just as directors and officers have a responsibility to ensure that the research and development lab door is locked and intellectual property is properly secured, today, it is increasingly clear that the same corporate governance responsibility exists with respect to security of company data, systems, and networks. The consequences of IT security breaches can be severe. It is now well substantiated that the theft of proprietary data and other cyber security breaches can result in a loss of market share, significant financial losses, or drop in market capitalization.[6]

Hacking, denial of service attacks, economic espionage, and insider incidents are commonplace and threaten the profitability of every business, leaving officers and directors vulnerable to lawsuits and civil and criminal penalties. Today, insider misuse of data and systems remains one of the top causes of security breaches, providing clear evidence that an area under the direct control of senior management and the board presents one of the highest risks to corporations. Indeed, last month, the U.S. Secret Service and Carnegie Mellon's CERT Coordination Center released an important study on insider threats in the banking and finance sector, noting that, "Management attention on financial performance, to the exclusion of good risk management practices, seems to be a recurrent theme in some of the cases in this study."[7]

Attacks coming from the outside – even those that do not involve theft, disclosure, or sabotage – present grave financial risks to corporations. An examination of the distributed denial of service attacks on Yahoo!, Amazon, and others in 2000 concluded that these attacks can result in a lack of confidence in the company and a drop in stock price.[8]

Any attack, whether from inside or outside the system, can damage the reputation of the company. The protection of a company's good name or brand is linked to a company's bottom line. Corporations have been reluctant to report cyber security breaches out of fear of damaging public relations and harming corporate reputation.[9] California has curbed this trend by enacting the Security Breach Information Act (SB 1386), a law that requires any state agency, person, or business that conducts business in California to notify the owner or licensee of information of any security breach of unencrypted personal information of any resident of California.[10]

---

[5] "Cybercrime," *Business Week*, Feb. 21, 2000.

[6] *See, e.g.*, "Companies urged to prepare for cyber attacks," *globalcontinuity.com*, Aug. 21, 2002, http://www.globalcontinuity.com/article/articleview/987/1/30/.

[7] *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* United States Secret Service and Carnegie Mellon CERT Coordination Center of the Software Engineering Institute, Aug. 2004 at 21, http://www.secretservice.gov/ntac/its_report_040820.pdf.

[8] A. Marshall Acuff, Jr., "Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business," Salomon Smith Barney, 2000, at 3-4, http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf.

[9] *Cybersecurity Today and Tomorrow: Pay Now or Pay Later,* National Research Council, Computer Science and Telecommunications Board, 2002, http://www7.nationalacademies.org/cstb/pub_cybersecurity.html.

[10] Security Breach Information Act (SB 1386), Feb. 12, 2002, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html; Devon Hewitt, "New California privacy law has nationwide ripple,"

Although California is ahead of the curve, the trend is clearly toward legislation requiring mandatory reporting of computer security breaches. At the federal level, Senator Dianne Feinstein has introduced Senate Bill 1350, "The Notification of Risk to Personal Data Act," modeled after the California reporting law.

Based on the foregoing, it is reasonable to conclude that directors and officers have a duty of care to protect a corporation's digital assets from a wide range of inside and outside security threats, to protect its market share and stock price from fluctuations as a consequence of these breaches, to guard its reputation, and to govern the conduct of employees. The degree of attention that is required to be given to these issues, however, falls within the Business Judgment Rule.

Business Judgment Rule

The majority of U.S. jurisdictions follow the business judgment rule that the standard of care is that which a reasonably prudent director of a similar corporation would have used. The business judgment rule "operate[s] as a shield to protect directors from liability for their decisions."[11] The ruling in one recent Delaware case turned attention to information systems and internal controls. The 1996 case, *Caremark International Inc. Derivative Litigation*, held that, "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under certain circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards."[12] To date, no shareholder suit has been brought against officers or directors for failure to take necessary steps to protect corporate systems and data, however, shareholders may have a valid basis for such derivative suits.[13]

The *Caremark* court noted that officer/director liability can arise in two contexts: (1) from losses arising out of ill-advised or negligent board decisions (which are broadly protected by the business judgment rule so long as the decision was reached out of a process that was rational or employed in a good faith effort) and (2) from circumstances where the board failed to act in circumstances where "due attention" would have prevented the loss. In the latter situation, the *Caremark* court noted that:

> [I]t would, in my opinion, be a mistake to conclude that . . . corporate boards may satisfy their obligation to be reasonably informed concerning the corporation, without assuring themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance. . . .

Washington Technology, July 7, 2003 at 12; Keith Poulsen, "California disclosure law has national reach," *SecurityFocus Online*, Jan. 6, 2003, http://online.securityfocus.com/news/1984.

[11] *Gries Sports Enterprises, Inc. v. Cleveland Browns Football Co.*, 26 Ohio St.3d 15, 496 N.E. 2d 959 (1986).

[12] *In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

[13] Jody R. Westby, "Protection of Trade Secrets and Confidential Information: How to Guard Against Security Breaches and Economic Espionage," *Intellectual Property Counselor*, (Jan. 2000) at 4-5.

> Obviously the level of detail that is appropriate for such an information system is a question of business judgment. . . But it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.[14]

The *Caremark* case could provide the basis for a shareholder suit against officers and directors for failure to implement an information and reporting system on the security of corporate networks and data such that the officers and directors could:

- Determine whether the organization was adequately meeting statutory, regulatory, or contractual obligations to protect certain data from theft, disclosure or inappropriate use; and
- Ascertain that the data critical to normal business operations, share price, and market share was protected.[15]

There are also high-risk situations where higher standards apply to directors and officers, such as acquisitions, takeovers, responses to shareholder suits, and distribution of assets to shareholders in preference over creditors. In these circumstances, directors and officers are required to obtain professional assistance or perform adequate analyses to mitigate the risks that ordinarily accompany these activities. Some information assurance experts assert that a "higher degree of care will also be required of Directors and Officers regarding the complex nature of issues involved in information assurance."[16]

Securities laws and regulations require public corporations to adequately disclose in public filings and public communications relevant risks to the corporation and its assets. The *Independent Director* put this in the context of information systems by reporting that:

> Management of information risk is central to the success of any organization operating today. For Directors, this means that Board performance is increasingly being judged by how well their company measures up to internationally-accepted codes and guidelines on preferred Information Assurance practice.[17]

Thus, the duty of officers and directors to make informed, good-faith decisions to protect the corporation's assets and financial stability is directly dependent upon the board ensuring that an

---

[14] *Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

[15] *See*, e.g., *id.*; For a general discussion on corporate liability related to board and officer responsibilities to ensure adequate information and control systems are in place, *see* Steven G. Schulman and U. Seth Ottensoser, "Duties and Liabilities of Outside Directors to Ensure That Adequate Information and Control Systems are in Place – A Study in Delaware Law and The Private Securities Litigation Reform Act of 1995," Professional Liability Underwriting Society, 2002 D&O Symposium, Feb. 6-7, 2002, http://www.plusweb.org/Events/Do/materials/2002/Source/Duties%20and%20Liabilities.pdf.

[16] John H. Nugent, "Corporate Officer and Director Information Assurance (IA) Liability Issues: A Layman's Perspective," Dec. 15, 2002, http://gsmweb.udallas.edu/info_assurance.

[17] *Id.* (citing Dr. Andrew Rathmell, Chairman of the Information Assurance Advisory Council, "Information Assurance: Protecting your Key Asset," http://www.iaac.ac.uk).

enterprise security program is in place that manages risks, sets policies and procedures for the conduct of employees and the operations of the corporation, and protects critical digital assets. Clearly, this duty cannot be met and informed decisions cannot be made if risk assessments are not performed.

Compliance with Legal Obligations

In addition to foregoing, officers and directors have a responsibility to ensure the company complies with legal obligations and requirements. Unlike the EU and Canada, which have omnibus privacy laws protecting personal information, the U.S. has a complex patchwork of privacy and security laws and regulations that apply to various industry sectors and types of information. Personal information can be protected by constitutions, laws, regulations, case law, and contracts between parties. At the state level, laws commonly protect arrest records and criminal justice data, bank records, cable television subscriber data, credit information, employment data, insurance information, mailing lists, medical and health data, polygraph results, school records, social security numbers, tax records, and telephone service and solicitation records. Federal laws protect all of the foregoing (except arrest records) plus Government data banks and wiretap information.[18]

In addition to compliance with non-disclosure agreements and other contractual or legal agreements, several recent laws enacted by Congress impose considerable privacy and security requirements on health information, financial information, and Government information and systems. They *each* require an enterprise approach to security, involving the senior management of the organization. Cumulatively, they impact a large portion of private sector systems. The three major laws directly impacting corporate security programs are:

- The Health Insurance Portability and Accountability Act (HIPAA);
- The Gramm-Leach-Bliley Act (GLBA); and
- The Federal Information Security Management Act (FISMA).

While not specifically mandating security measures, the Sarbanes-Oxley Act of 2002 is also drawing attention to information security programs. Critical infrastructure (CI) industries also live under a veiled threat of regulation due to inadequate security programs.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) protects "Individually Identifiable Health Information" and imposes extensive privacy and security regulations on health care providers, claims processors, insurance companies, and businesses.[19] By extension, HIPAA also applies to "business associates" of covered entities.[20] HIPAA's privacy and security requirements are quite broad. Section 1320d-2(d)(2) of HIPAA states:

---

[18] *Privacy Laws by State* (excerpted from *Compilation of State and Federal Privacy Laws*, 1997 ed., by Robert Ellis Smith and *Privacy Journal*), http://www.epic.org/privacy/consumer/states.html.

[19] Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191, 42 U.S.C. § 1320d, http://www.hipaadvisory.com/regs/law/index.htm (hereinafter "HIPAA"). Information on HIPAA privacy, security, and electronic transaction regulations can be found at http://www.hipaadvisory.com/regs/index.htm.

[20] 45 C.F.R. § 160.103 (definition).

> Each [covered entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards –
>
> (A) to ensure the integrity and confidentiality of the information;
> (B) to protect against any reasonably anticipated –
> (i) threats or hazards to the security or integrity of the information; and
> (ii) unauthorized uses or disclosures of the information; and
> (C) otherwise to *ensure compliance with this part by the officers and employees of such persons.*[21]

The regulations, however, can be quite granular. HIPAA's Security Regulation covers data while both in storage and transit and has 28 "standards" and 41 "implementation specifications." There are administrative, physical, and technical aspects to the rule. The rule requires that an enterprise approach be taken with policies, procedures, change control mechanisms, risk analysis, review, and training.[22] The Security Regulation takes into account technical capabilities of record systems, costs of security measures, the need for personnel training, and the value of audit trails in computerized record systems.

HIPAA compliance concerns are backed up by criminal penalties. Wrongful disclosure of individually identifiable health information carries up to a year in prison and up to a $50,000 penalty. If the wrongful disclosure is under false pretenses, the maximum term rises to five years, and the monetary penalty to $100,000; add an intent to sell, transfer, or use for commercial advantage, personal gain, or to inflict malicious harm, and the prison term increases to a maximum of 10 years, with a monetary penalty of up to $250,000.[23]

Gramm-Leach-Bliley Act (GLBA) and Financial Guidance

The Gramm-Leach-Bliley Act (GLBA),[24] states that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[25] The GLBA definition of "financial institutions" encompasses banks, securities firms, insurance companies, and other companies providing many types of financial products and services to consumers. This includes lending, brokering or servicing any type of consumer loan; transferring and safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts; and other types of financial

---

[21] HIPAA, 42 U.S.C. § 1320d-2(d)(2) (emphasis added).
[22] Linda A. Malek and Brian R. Krex, "HIPAA's security rule becomes effective 2005," *The National Law Journal*, Mar. 31, 2003 at B14; *see also* Chapter Five, Security Plans, Policies & Procedures.
[23] HIPAA, 42 U.S.C. § 1177(b).
[24] Gramm-Leach-Bliley Act of 1999, Pub. Law 106-102, 113 *Stat.* 1338 (1999), http://www.ffiec.gov/ffiecinfobase/resources/management/con-15usc_6801_6805-gramm_leach_bliley_act.pdf (hereinafter "GLBA").
[25] GLBA, 15 U.S.C. § 6801, http://www4.law.cornell.edu/uscode/15/6801.html.

services.[26] GLBA's definition of financial institutions has even swept up colleges and universities.[27]

Pursuant to the GLBA, the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Federal financial regulatory bodies[28] have issued regulations requiring administrative, technical and physical safeguards for financial information. The statute specifies that the regulations are intended:

1) To ensure the security and confidentiality of customer records and information;

2) To protect against any anticipated threats or hazards to the security or integrity of such records; and

3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[29]

The regulations set forth the required steps that must be taken, but they do not specify what the technical components of a safeguards program must be. For example, the Federal Trade Commission requires that financial institutions under its purview must develop a plan in which the institution must: (1) designate one or more employees to coordinate the safeguards, (2) identify and assess the risks to customers' information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks, (3) design and implement a safeguards program, and regularly monitor and test it, (4) select appropriate service providers and contract with them to implement safeguards, and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firms business arrangements or operations, or the results of testing and monitoring of safeguards.[30]

In addition to GLBA, there are also standards and guidance for financial system security. The Federal Financial Institutions Examination Council's (FFIEC) *IT Examination Handbook* sets forth an enterprise and process approach to information security. This follows the same approach the FFIEC took in its "Guidelines to Establishing Standards to Safeguard Customer Information" regarding implementation of the GLBA.[31] In addition, the Office of the Comptroller of the Currency (OCC), which regulates and supervises national banks, has formally advised banks to safeguard against the threats and vulnerabilities of cyber terrorist attacks.[32]

---

[26] "Financial Privacy: The Gramm-Leach Bliley Act," http://www.ftc.gov/privacy/glbact/.

[27] "Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information," *NACUBO Advisory Report 2003-01*, National Association of College and University Business Officers, Jan. 13, 2003, http://info-center.ccit.arizona.edu/~security/GLBA_Summary.pdf.

[28] The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, and the National Credit Union Administration.

[29] GLBA, 15 U.S.C. § 6801, http://www4.law.cornell.edu/uscode/15/6805.html.

[30] *See* "Financial Institutions and Customer Data: Complying with the Safeguards Rule," http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[31] FFIEC Examination Handbook at 1.

[32] *See* "Infrastructure Threats from Cyber-Terrorists," Office of Comptroller of the Currency, OCC 99-9, Message to Bankers and Examiners, Mar. 5, 1999, http://www.occ.treas.gov/ftp/bulletin/99%2D9.txt.

The World Bank also has been a leader in the area of financial security of electronic transactions. Through a series of papers, reports, presentations, and events, The World Bank has made a global contribution toward "connecting the dots" in the security of financial transactions.[33] The Bank's *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues* sets forth "The 12 Layers of Security,"[34] which has been implemented by The World Bank Treasury, incorporated in the Monetary Authority of Singapore's Risk Management Guidelines, and added to the latest ISO Information Security Banking Standard 13569.[35]

Federal Information Security Management Act (FISMA)[36]

Title III of the E-Government Act of 2002, also known as The Federal Information Security Management Act (FISMA), added several requirements for the security of Government systems.[37] FISMA also applies (1) to private sector contractors who process Government information or operate systems on behalf of the Government, and (2) when Federal information is used within equipment that is acquired by a Federal contractor incidental to a Federal contract.

Under FISMA, the term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability of information.[38] FISMA requires the head of each Federal agency to provide certain information security protections for agency information and systems and to ensure that information management security processes are integrated with agency strategic and operational planning processes.

Taking an enterprise approach, consistent with security best practices, FISMA requires the head of each agency to develop, document, and implement an agency-wide information security program to provide security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity. This includes:

---

[33] *See, e.g.*, Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Public Policy Issues, The World Bank, June 2002, http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationversion3/$FILE/E-security-Risk+Mitigation+version+3.pdf* (hereinafter "Glaessner, Kellermann, and McNevin"); Thomas Glaessner, Tom Kellermann, and Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions—Summary of Recent Research and Global Dialogues*, The World Bank, May 2003, http://www.worldbank.org/wbi/B-SPAN/sub_e-security.htm (hereinafter "World Bank Financial Security Summary").

[34] Glaessner, Kellermann, and McNevin at 51-52.

[35] An updated version of ISO/TR 13569 which incorporates the 12 Layers of Security will be released mid-2003, *see* http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=13569.

[36] This portion of the testimony is taken from a section of Westby – Cyber Security (pp. 49-54) of which I own the copyright.

[37] Federal Information Security Management Act, Title III of E-Government Act of 2002, Pub. Law 107-347, http://csrc.nist.gov/policies/FISMA-final.pdf (hereinafter "FISMA").

[38] 44 U.S.C. § 3542.

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems;

- Policies and procedures that are based on the risk assessments and ensure compliance with security guidance and standards;

- Security awareness training to inform personnel, contractors, and other users of information systems that support the operations and assets of the agency of:
  (a) information security risks associated with their activities; and
  (b) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

- Periodic testing and evaluation (not less than annually) of the effectiveness of information security policies, procedures, and practices, which includes testing of management, operational, and technical controls;

- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

- Procedures for detecting, reporting, and responding to security incidents; and

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Sarbanes-Oxley Act of 2002

Although the Sarbanes-Oxley Act of 2002[39] does not specify information security measures, it does require officers of public companies to attest to the appropriateness and integrity of the financial data reported in SEC filings[40] and to assess and report on the effectiveness of the internal control structure and procedures for financial reporting.[41] In today's business environment, financial data is digital and processed and stored in a variety of ways. Therefore, the legal requirements of Sarbanes-Oxley are directly dependent upon the integrity of the IT systems processing the data.

Critical Infrastructure

Section 2 of the U.S. Homeland Security Act defines "critical infrastructure" (CI) as having the same meaning as that used in the USA PATRIOT Act:

[39] Sarbanes-Oxley Act of 2002, Pub. Law 107-204, § 302, http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (hereinafter "SOX").
[40] SOX, § 302.
[41] SOX, § 404.

> [T]he term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the ... [nation] that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The National Strategy for Homeland Security, released by the White House on July 16, 2002, lists the following as critical infrastructure:

- Agriculture
- Food
- Water
- Public health
- Emergency services
- Government
- Defense industrial base
- Information and telecommunications
- Energy
- Transportation
- Banking and finance
- Chemical industry and hazardous materials
- Postal and shipping.

The Administration has grown increasingly nervous about the fragility of our nation's critical infrastructure and the lack of attention from boards and senior management to fully engage on the security of these infrastructures, including their supervisory control and data acquisition (SCADA) and supporting IT systems. To that end, the Administration issued the *National Strategy for the Protection of Critical Infrastructure and Key Assets*[42] and the *National Strategy to Secure Cyberspace*[43] identifying the key measures that need to be taken to ensure these assets are available when needed and secure from attack. Subsequently, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which establishes a national policy for Federal departments and agencies to identify and prioritize CI and key resources and protect them from terrorist attacks.[44] Although there are no mandated requirements for the security of critical infrastructure, there have been repeated warnings that the Administration would ask Congress to enact legislation requiring comprehensive security programs if senior management did not step up to the plate.[45] HSPD-7 makes regulation that much easier and provides a

---

[42] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Mar. 4, 2003, http://www.whitehouse.gov/pcipb/physical.html.

[43] *The National Strategy to Secure Cyberspace*, Feb. 14, 2003, http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

[44] Homeland Security Presidential Directive / HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection," Dec. 17, 2003, http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

[45] *See, e.g.*, Martin Edwin Anderson and Tim Starks, "Government and Industry Struggle to Build a Post-9-11 Partnership," *Congressional Quarterly Homeland Security*, 2004, http://www.ewa-iit.com/content.asp?sectionID=6&contentID=137; Michael Singer, "National Cyber Security Initiative Still Stalling," *eSecurityPlanet.com*, Dec. 3, 2003, http://www.ewa-iit.com/content.asp?sectionID=6&contentID=137.

legitimate justification for doing so in the name of national and economic security and public safety.

Situation Today

Senior executives of an organization should regard cyber security as a management opportunity rather than a technical problem. The good news is that a number of factors are moving companies toward the development of robust security programs. Two of the most obvious are increasing connectivity and raised awareness regarding (1) vulnerabilities and threats and (2) the availability of best practices, standards, and guidance.

In addition, some excellent reference materials have been developed that guide directors and officers through the digital governance process. The *International Guide to Cyber Security* sets forth a comprehensive list of non-technical, *management* questions in the areas of assessment, security program, internal controls, implementation, and compliance and enforcement.[46] Of course, the heightened emphasis on corporate governance and the responsibilities of executives to take action to protect market share, stock price, and corporate reputation is also helping.

Now the bad news. There is a growing knowledge base and evidence of:

- Collaboration between terrorist organizations and organized crime in the areas of drug trafficking, money laundering and other forms of financial crime, and weapons trafficking, among others. Identify theft can play a significant role in all of these crimes.[47]

- Terrorists' use of IT to communicate and conspire on attacks against critical infrastructure. In fall 2001, the Mountain View, California, police department requested FBI assistance in investigating suspicious surveillance of computer systems controlling utilities and government offices in the San Francisco Bay Area. The digital snooping was being done by Middle Eastern and South Asian browsers. The FBI found "multiple casings of sites" through telecommunications switches in Saudi Arabia, Indonesia, and Pakistan that focused on emergency telephone systems, electrical generation and transmission equipment, water storage and distribution systems, nuclear power plants, and gas facilities across the U.S. Some of the electronic surveillance focused on the remote control of fire dispatch services and pipeline equipment. Subsequently, information about those devices, including details on how to program them, was found on Al Qaeda computers seized this year.

  The U.S. Government has expressed concern that terrorists are targeting the junctures between physical and virtual infrastructures, such as electrical substations handling hundreds of thousands of volts of power or panels controlling dam floodgates. According to a recent *Washington Post* report, one Al Qaeda laptop found in Afghanistan had frequented a French website that contained a two-volume online

[46] Westby – Cyber Security at 194-96.
[47] *See, e.g.*, "The Fusion Task Force," Interpol, Sept. 20, 2004, http://www.interpol.com/Public/FusionTaskForce/default.asp.

"Sabotage Handbook" on tools of the trade, planning a hit, switch gear and instrumentation, anti-surveillance methods, and advanced attack techniques. An Al Qaeda computer seized in January 2002 in Afghanistan contained models of a dam, complete with structural architecture and engineering software that enabled the simulation of a catastrophic failure of dam controls. Other computers linked to Al Qaeda visited Islamic chat rooms and had access to "cracking" tools to search networked computers and find and exploit security holes to gain entry or full command. Additionally, evidence obtained from browser logs indicate Al Qaeda operatives spent time on sites that offer software and programming instructions for digital switches that run power, water, and transport and communications grids. Al Qaeda prisoners have reportedly admitted to planning to use such tools. These systems are especially vulnerable because many of the distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems that control critical infrastructure are connected to the Internet but lack even rudimentary security. In addition, the technical details regarding how to penetrate these systems are widely discussed in technical fora, and experts consider the security flaws to be widely known.[48]

- Cyber incidents that cascade and domino through systems, affecting, and possibly endangering, millions of people.[49]

- The inability or difficulty to track and trace cyber incidents. The original engineering of the Internet did not anticipate that it would support the global economy and link businesses and process transactions. The Internet was designed for a trustworthy population of scientists and researchers and, therefore, did not originally incorporate the ability to track and trace user behavior. For example, Internet Protocol (IP) addresses can be readily "spoofed" by attackers to hide their true source of attack. Due to the poor state of security throughout the Internet, computers are easily taken over by attackers and used as "stepping stones" to hide their tracks or amplify their attacks. Also, a large number of IP addresses are dynamically assigned, requiring extensive cooperation among Internet Service Providers (ISPs) and law enforcement when trying to track and trace incidents to actual individuals. Even when tracing is possible, if a packet has been routed through a foreign country or if the perpetrator is located overseas, jurisdictional issues are burdensome and time consuming, international cooperation of law enforcement may be difficult or impossible, and any search and seizure of evidence may be performed in a manner that renders it inadmissible in a U.S. court.[50]

In light of the foregoing, it is hard to conceive that conducting risk assessments and following best practices would increase a company's risk of liability. In fact, the contrary conclusion is

---

[48] Toward a Universal Order of Cyberspace at 10 (citing " Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 26, 2002, http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html)

[49] Jody R. Westby, "Cyber Realities: From Worms to Warfare," NATO Forum on Business & Security, Berlin, Feb. 2004.

[50] Jody R. Westby, ed., *International Guide to Combating Cybercrime,* American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2003, http://www.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030.

apparent: boards and senior management who wish to ignore digital governance and risk management actually *increase* the likelihood of corporate and personal liability in the event of a cyber incident.

Solving the Problem

Some corporations may ask their counsel to conduct any risk assessments performed, hoping to protect it under the cloak of attorney work product.[51] This privilege can provide some degree of protection from disclosure of certain audit or risk assessment information when specific conditions are met. Generally, the attorney work product privilege established in *Hickman v. Taylor*,[52] protects from disclosure materials prepared by attorneys "in anticipation of litigation." Such work product includes an attorney's thoughts, litigation plan or strategy, evaluation of facts and evidence, and legal theories relevant to his client's case.[53] However, the "anticipation of litigation" requirement places a significant limitation on this privilege.[54] "[A]t the very least, some articulable claim, likely to lead to litigation, must have arisen."[55] Thus, it is not likely that this privilege will afford substantial protections.

I tend to favor market solutions over regulation. I believe there are approaches open to Congress that would both motivate the private sector and result in dramatic improvements to our computer systems and networks. The most obvious solution is to provide tax credits to corporations that implement enterprise security programs. Such credits could encompass risk assessments, implementing best practices and standards, establishing internal controls, integrating security into the capital planning and investment process, and training. Another initiative could provide Government grants or funding to academia, private sector entities, and our national laboratories to help advance the development of models to effectively measure return on investment of security programs and other tools that would help boards and senior management through the decision-making processes regarding cyber security.

Lastly, I would like to draw the Subcommittee's attention to the three books recently published by the American Bar Association's Privacy & Computer Crime Committee: The *International Guide to Combating Cybercrime* (2003), the *International Guide to Cyber Security* (2004), and the *International Guide to Privacy* (2004). The *Roadmap to an Enterprise Security Program* will be published within the next month. These books dovetail the legal, technical, managerial, and operational aspects of privacy, security, and cybercrime and guide the reader through the development of an enterprise security program.

---

[51] *See generally,* Westby Cyber-Security at 244-46.
[52] *Hickman v. Taylor*, 329 U.S. 495 (1947) (codified as Federal Rules of Civil Proc. P 26(b)(3).
[53] *Id.* at 510.
[54] *Coastal States Gas Corp. v. Dep't of Energy*, 199 U.S. App. D.C. 272; 617 F.2d 854, 864 (1980). State law, however, may differ on this rule. For example, under California Civ. Proc. Code 2018, there is not mention of the "anticipation of litigation" requirement and California courts have ruled according to this statute that the privilege also applies to the work product of an attorney when he acts as counselor in a nonlitigation capacity. *See Casualty & Surety Co. v. Superior Ct,* 153 Cal. App. 3d 467, 478-479 (1984); *Rumac, Inc. v. Bottomley*, 143 Cal. App. 3d 810, 815-16 (1983).
[55] *Id.* at 864.

The books were written by an international, multidisciplinary team of technical experts, attorneys, industry representatives, government officials, NGO representatives, and members of academia. We recognize that our national and economic security and the protection of our citizens from an array of threats, ranging from identity theft to terrorist attacks on critical infrastructure, is, in part, dependent upon the security of the networks in the nearly 200 countries connected to the Internet. Our ability to prosecute cybercrimes is dependent upon trained law enforcement and prosecutors and inter-governmental cooperation in those 200 countries. Our ability to protect private information is also dependent upon our ability to guide developing countries toward good cyber security practices, laws, and policies.

To that end, the ABA is making all four of these publications available free of charge to persons in developing countries. The *Cybercrime* book has already been translated into one language, and we hope to obtain funds for the translation of all the publications into Russian, Spanish, and Chinese so they might reach a global audience through workshops and their use as textbooks. Congressional funding for these types of translation and workshop efforts would significantly increase our ability to combat cybercrime and secure our networks against catastrophic or costly attacks.

Mr. Chairman and Members of the Subcommittee, I thank you for your consideration and this opportunity.

Mr. PUTNAM. Mr. Schmidt and Mr. Conner, through your extensive work on information security issues, what conclusions have you drawn about why corporate America is not taking the problem with information security seriously enough?

Mr. SCHMIDT. Well, I am not sure that I totally agree that it is not being taken seriously. I think, as has been pointed out more than once, there is a greater recognition now more so than ever before of the tremendous importance that cybersecurity is, but it is very complex. It is not as if we designed a system to eventually become secure. Many corporations that I see literally around the world have built systems that they put a system in place, and then they add another piece on top of it, so it has been very difficult.

What happens in the past couple years, now we recognize obviously the critical infrastructure protection piece and the governance pieces, as Mr. Conners related to, where we have seen a lot more intended dollars and efforts put into the cybersecurity. But it is a complex issue, and is not something you can just flip a switch and turn it over. It will take a couple years by the time we get operating systems and engineering design and quality processes in place to make it be able to respond and say, yes, we have much better security now than we have in the past.

Mr. PUTNAM. Mr. Conner.

Mr. CONNER. Simply, they are not taking the time. And if you take the time, the question is where you start. That is why we spent considerable amount of time on a framework, because I personally believe, as many companies do, you need a framework to systemically assess your business for where the high risk is and how do you get a baseline to measure it. Once you have that, then you can apply it. It is a very simple process to get started, but if you don't know where to start, all your journeys will take you somewhere, but maybe not where you want to go, and you won't get a return on investment, and you won't be more secure.

I think that starts with the senior management executives and board saying, we are going to take a framework that exists now, it is public, it has been there for 6 months, and get started. And that means you can't delegate it to a CIO; you have to assess your own business needs and risks. And that is something in today's environment; many corporations do it, and many more don't do it. And I can assure you, in the ones I talk to, all of them are concerned about the liability of that assessment. It is a litigious society, and in this environment with class actions and others, that evidently comes through every discussion.

Mr. PUTNAM. Dr. Hancock, do you wish to add anything to that?

Mr. HANCOCK. I have two perspectives on it, sir. One is I deal with the same folks that Mr. Schmidt and Mr. Conner deal with in many respects because a lot of us all have the same kind of customers. It has been my experience that most board of directors-level folks have a very limited knowledge of security, and a lot of that is because security is not personal to them. They don't understand even the basics.

And I will give an example, sir. My son is 15 years old. When he was 7 years old, someone tried to kidnap him. Because I am a security person and by definition paranoid, when he started—at 4 years old I started him in Taikwando. When the person grabbed

my son, my son dislocated his kneecap and four of his knuckles. As a result of that, I believe that assets should be self-defensible, and includes my family, includes my children, includes my home, whatever the case may be.

Most people don't look at security that way. To them, security is managed and dealt with by someone else, and, just like Mr. Conner said, a lot of times delegated to the CIO. Many times the CIO has no capabilities or understanding of what the security issues are. It is chopped out of the budget. It is considered to be something that is more of an irritant than something that needs to be done.

So it's not part of the corporate agenda overall. The second problem runs in, just from a pure technology perspective. Very few people in the business really understand how to secure things correctly. One of the problems we have is we continue to deploy technologies that are not secure in nature, and then we go back and try to provide technology to secure that.

As a case in point in my own company, I operate well over 50,000 routers. Of those 50,000 routers, I have over 11,000 firewalls. I know categorically that those firewalls cannot protect my network or my customers from everything that will come by, because the oppositions are far more creative and have a lot more time than my security people do.

As a result of that, we are in a constant challenge from a pure security perspective. How do you stop things from happening when the technology doesn't exist for us to identify who is launching an attack or identify a way for us to go back and trace it back to figure out where it is coming from, just the very basics? So you have a secondary problem that if the board of directors did come down tomorrow and they did embrace security and said, yes, really want to do this, the sad reality is much of the technology that is required to stop a lot of this nonsense from happening just flat doesn't exist, and it will take time for that technology to be put into place since it is going to take research to make happen.

Mr. PUTNAM. Thank you. My time has expired. I will call on Mr. Clay.

Mr. CLAY. Thank you. Ms. Westby. I will start with Ms. Westby. First of all, thank you for your publication, and can you tell me what lessons can be learned from the private sector's efforts to comply with the internal control requirements of the Sarbanes-Oxley legislation by the Federal agency community? Are there similarities between the public and private sectors in terms of securing networks containing vast amounts of individual data?

Ms. WESTBY. Actually, I think that the private sector in this instance learns more from the government. Information security is very different from the days when Al Gore was reinventing the government and the government was looking to the private sector for best practices.

Our government is clearly the world leader in information security practices, and NIST has done world-class work. Their guidance and controls in metrics is excellent, and they, the enterprise security program mandated by FISMA and the NIST guidance that corresponds with that, offer an excellent example.

It is unfortunate that the word "security" is not mentioned anywhere in Sarbanes-Oxley, and there is a lot of traffic on my

listserves about what does that really mean, what do the internal control requirements really encompass and how far does that go into checking integrity of financial data, how far does that goes into systems.

Mr. CLAY. Thank you for that response.

Mr. Schmidt, as a former White House Cyber Security Adviser, would you agree that the Federal procurement process would be an ideal mechanism to improve the security of products and services delivered by vendors to the agency community? Wouldn't this have a profound effect on the development of more secure and uniform products for both the agency and critical infrastructure and communities?

Mr. SCHMIDT. Yes, sir, I sure do. As a matter of fact, I talked from time to time about discussions we have had with vendors that supply service to the government and CIO, CSOs for the government, and it was amazing the disconnect that I have seen many times where, say, listen, we would like to actually pay extra money to get security services, but nobody is willing to provide it. And then you go to the vendor, vendor says nobody is willing to pay the extra money for it.

So clearly the procurement arm of government can do much to, you know, set requirements, instead of, you know, accepting things the way they are, establish the requirements that one would have, and then that will have that trickle down effect to the rest of society, because if we are buying more secure routers and more secure operating systems for the government private sector is clearly going to jump on that bandwagon as well. So it's a vehicle I think can take us a long way in a short period of time.

Mr. CLAY. Let me ask you, according to Mr. O'Carroll, from our first panel, the SSA's Office of Inspector General had recently discovered a plan by one individual to sell up to 10,000 Social Security numbers and matching names on your company's Web site.

Can you outline for us the methods and controls utilized by your company to identify and prevent such illicit activity?

Mr. SCHMIDT. Yes, we do. We have an entire group, literally hundreds of people worldwide, that look at listings that occur for everything from counterfeit currency to, you know, war materiel, weapons, things of that nature, and we have not only physical reviews of data but also automated reviews.

Various trigger mechanisms will actually flag something for the customer service people to dig down further into it. The challenge we run into from time to time is that people get very, very creative about how they title certain things. So they may not cite it saying, well, I am going to sell Social Security numbers but they are going to say identification cards, which may not trigger something. So we are constantly evolving and changing to make sure we that we adapt to the things that we see out there as new threats occur.

Mr. CLAY. Thank you for that response.

Mr. Chairman, I yield back my time. I have no further questions.

Mr. PUTNAM. Mr. Clay, thank you.

Ms. Westby, from your testimony, and you have heard the answers that the other panelists have given about this issue, the issue of ignoring information security risks and the liability that it avoids or causes, in your experience in the field of information

technology law, do you see the attitude of being proactive about information security taking hold?

Ms. WESTBY. Yes. The market has matured. The awareness has increased, and I believe that especially in the environment we have today, with heightened emphasis on corporate governance, that senior management and boards are taking a look at what exactly is within their realm of responsibility, and they, at least many of the major companies who are assisting with Sarbanes-Oxley, are saying we have to look at how you are handling the data in the computer system. I think overall, though, our efforts have been in vain.

Over the last 6 years there have been enormous efforts made by the Federal Government, by different organizations, to engage businesses through, as an enterprise, horizontally and vertically across an organization. I do think that has matured and that we are seeing progress.

Mr. PUTNAM. Thank you. Mr. Schmidt and Dr. Hancock, in your lines of business, clearly spam and denial of service attacks are of great concern. A recent Symantec report suggests that for the first half of this year it saw a huge increase in zombie PCs. The company said it was monitoring 30,000 per day. You made reference to that, Dr. Hancock, with a peak of 75,000. Some estimates state that it is possible that as many as half of the machines on the Internet are in an infected state.

How big of a threat is this bot issue or zombie issue to national or economic security?

Mr. SCHMIDT. Well, I couldn't agree more. We have seen instances, in working with the law enforcement folks, those exact numbers—we have actually been able to identify from cable modem and home DSL users. So it's significant, because if you look through the cascade of litanies and ills that can result as a result of that, one clearly the hacking portion into the critical infrastructure, the identity theft, the denial of service attack capability.

If you remember back, February 2000, when we had the big denial of service attack that people talked about all the time, that was done at a rate of about 800 megabytes per second, which is a relatively insignificant amount of data now. Now, with 20,000 systems that have been compromised, you can do 3 gigabytes, you know, almost three times as much worth of damage. So when you look at the overall aspect of it, you look at the identity theft, you look at the lack of trust that we have in the environment, if 87 percent of that 840 million users I referenced to earlier, are doing e-mail, less than 17 percent are doing e-commerce, economically that's just as bad. We should be able to go ahead and improve that. The way we can go ahead and do that is by making sure that we have the defense in depth where, No. 1, the spams and cams aren't getting in the inbox for the most part. If they do get there, some sort of firewall or browser protection or some sort of file validation keeps you from doing something ill from there; and then last of course making sure that we are getting a law enforcement prosecution of these things.

The challenge I have with the law enforcement side, which is directly related to this, is this is a crime in progress. This is no different than somebody walking into a liquor store and sticking up

somebody with a gun, except you are not there physically. It has to be dealt with on a real-time basis.

Mr. PUTNAM. Dr. Hancock.

Mr. HANCOCK. I will have to agree with Mr. Schmidt on all of that. I will also add that one of the problems we have with zombie networks is that many times that we found over the last few years—is that those zombie networks are now being operated by organized crime in some cases.

As a matter of fact, there was one I was recently involved with—a direct investigation on—that was a gaming site, where the gaming site was held up for extortion because of a denial of service attack launched against it by a series of Russian organized crime. We know that. We tracked it back. We worked with the Russian law enforcement agencies. The fact of the matter was we pinned it down and nailed the guy. But the situation is that it took months to happen.

This sort of thing is happening more and more. We are seeing a whole lot more happening where e-commerce is the reason for the site to exist. And we are seeing more and more of this happen where corporations are depending more on their network infrastructure and then they are being held up for extortion or being held up for some sort of, if you will, ransom because of their technology being disabled through things like denial-of-service attacks and things like zombie nets being used.

I will also agree with Mr. Schmidt—what he just said—about the severity of these types of attacks. We recently saw a denial-of-service attack execute a 3.2 gigabytes. I had not seen one like that before. We operate a very large network infrastructure. We have a lot of customers out there that are some of the places that you would normally frequent on the Web.

When that one hit we disabled that one within 6 minutes. But what was more important about it was within 5 minutes after that the attacker completely redirected and attacked a completely different addressing block. I have never seen something like that happen. That means you can take 10,000 to 20,000 zombies, literally have them turn on a dime, and then reconnect and reattack a completely different site.

That basically shows technical sophistication on the part of the attackers. It also shows that the zombie sophistication is increasing, which means that these products can be directed, redirected very, very quickly, and be pointed with a very debilitating attack against a very large network pipe. As a result of that, over time we are going to see more of that happen, where the zombie networks where we have 5,000, 6,000 zombies all of a sudden become 100,000. And now the types of attacks that can kill things like power networks, water networks, those start to become very serious reality, where a whole power grid is disabled simultaneously.

So I believe that the zombie threat is a very severe one. I think it's going to get a lot worse, just like any other software. There are new versions of it coming out all the time and the zombies are being upgraded with additional capabilities. All of these things put together are going to cause very serious problems to our e-commerce capabilities.

Mr. PUTNAM. Who has the sophistication and technical capacity to do what you just described?

Mr. HANCOCK. If you asked me that question 10 years ago, I would have to say it would be a hard core, stone geek to do it. The fact is any more it takes very little sophistication. The attack Mr. Schmidt talked about in February 2000 was my first day of employment at the company that was acquired—and then acquired where I am now. I had been with the company exactly 2 minutes when Amazon.com, CNN.com and a few other sites went splat. The realty of that was we found out later in the day those attacks were executed by a 16-year-old out of Toronto, Canada who went by the handle called Mafia Boy.

We were involved with the FBI and with the Secret Service and quite a few other agencies to track this individual down. We are capable of tracking these people down fairly quickly. Trying to get them apprehended and dealt with is a different story. That took weeks.

So the end result was you had a child here who downloaded an "exploit" from a Web site. This individual had no sophistication whatsoever in understanding that exploit or in writing that tool. However, sophisticated people are all over the Web. Those sophisticated people will find the vulnerability. They will write the exploit. They will post it on a Web site. They themselves do not execute that particular attack. Instead, other people—which we call script kiddies, 13 to 18-year-old types—will download and execute debilitating attacks. This is very, very common and compromises approximately 80 percent of the attacks we see.

My infrastructure gets attacked anywhere from 200 to 400 times a day. As a result of that, we see a lot of this stuff. We deal with a lot of that stuff. Most of the time it is pretty straightforward to deal with it.

What I am concerned about is the people who are serious, doing it for profit motives. Those people will employ programmers—they will employ people with specific skill sets—and those people with specific skill sets will create these tools for a specific nation reason. There may be a nation state that wishes to cause harm to us by debilitating capabilities or somebody just as simple as a Russian mob trying to go back and extort money from a company that executes business over the Web.

Mr. PUTNAM. What responsibilities does the hardware and software community have in all of this? How much does the constant influx of new patches for vulnerabilities in their products contribute to the problem of cyber crime?

Mr. HANCOCK. Well, sir, I will give you an example, a very popular desktop operating system that's floating around, used to have a version called Version 3 that comprised 3 million lines of code. The current version, which was very popular on most PCs, comes out with over 45 million lines of code. The next version coming out next year is going to be b almost 50 million lines of code.

When you have something that large, trying to secure that, no matter how conscientious you are, is virtually impossible. And so the result is as our versions get more and more sophisticated, as they get more and more and more complex and we layer complexities on top of that operating system—for example, a very popular

data base out there has almost 1 billion codes in it. When you take an operating system that has 45 billion lines of code, a data base with 1 billion lines of code, you then put on top of that object-oriented programming, which is done by the programmer so that you can communicate to the data base, so you can do something useful with it, you can end up very quickly with a couple of billion lines of code on a server sitting in a data center someplace. Trying to secure that is not trivial. Trying to go back and instill programming discipline to make that secure is not trivial.

All of these things require a great deal of education on the part of programmers. They also require standards. They also require other types of methodologies that say this is a good way to write code or a bad way to write code. The problem that we have is that we have gone and put all these types of technology in for many years without any discipline in the areas of security, all from the way our program is written to the way that we deploy technology to the way we manage it on a day-by-day basis. And just like when Mr. Conner said and Ms. Westby said and Mr. Schmidt have said—a lot of it has to do with corporate governance. There has not been an insistence by the corporate echelon to require vendors to instill security in their technology, to put security in, code, to put security in even simple things like routers.

My most basic concern is that I work very closely with all the chief security officers of the telcos through the FCC. We offer something there called Focus Group 2B, which puts forth cyber security best practices. There are 54 people involved with that. We own about 90 percent of the actual infrastructure that everybody uses.

We got together last December and told the FCC categorically, and through public documentation, that one of the biggest problems we have is we are keeping to deploying technology which is woefully inadequate, and we keep deploying more.

So to give you part of an example of a zombie problem, one of my base concerns that keeps me awake right now is third generation cell phones, and that is because most cell phones coming out of the cell phone manufacturers operate an operating system which is a derivative of Linux. That operating system can have viruses. That operating system can be used as a zombie. Under third generation cell phones they will all have a TCP-IP address. This means that every single handset can become a zombie and part of an attack vector, which means the current population of approximately 850 million Internet nodes will grow very quickly to 3 billion Internet nodes, all of which can be attacked and put through worm automation technology, a zombie parked on every handset out there.

In addition, those handsets will be used for everything from e-commerce to charge services, to go back over and even get a soda out of a soda machine, because they are all being done that way in Europe right now. All those areas basically mean that the software development, the hardware development, has to instill security discipline, which is not there. In addition to that, we will continue to deploy these technologies, and these technologies have serious flaws in them. That is not being corrected.

Mr. PUTNAM. That's uplifting.

Mr. Schmidt, you made reference to the fact that simply using passwords is just not adequate any more and that the Nation should move to a two-factor authentication by the end of next year. Yesterday a major ISP announced that it would make major authentication available to its customers. Do you see this as being a positive development, and do you see that being the beginning of even more offerings of and a greater commitment to secure communications?

Mr. SCHMIDT. Yes. As a matter of fact, it's a tremendous step forward. We have been working for about the past 7 months. We, meaning a group of security experts, have been working with that company, other companies, Mr. Conner's company, others, looking for solutions that we can do on a real-time basis to provide that extra two-factor authentication for the customer and end user space. I cite my DOD side of life as a computer crime investigator. I now have a spy card I can use on my computer government system that I can log into my DOD account with full encryption, full authentication, and to really know it's me.

We need to move that way in a security space for the consumers. It's probably going to be a slow process. There's going to be some shaking up of who is going to be the coalition and who is doing this. I think we have clearly reached a point in society with the phishing e-mails, the identity theft, the hacking, that society is ready to move to the ATM card of online world, if you will.

Mr. PUTNAM. Mr. Conner, do you see other companies following AOL's lead?

Mr. CONNER. Yes. The only comment I made, and Howard and I talk about, it's a necessary step but it's a baby step. Most of these are cost prohibitive for the masses, and this is not an issue that can be dealt with on the haves and have-nots. That is going to require innovation and deployment around identity and how do you deal with identity for every citizen or customer of eBay or someone else. And the current technology, that becomes quite cumbersome to do in terms of ease of use and economics.

I would also offer it's only half the issue. Authentication or identity is one-half. It's the information they are reaching for that is the other half, and the second factor of any authentication scheme only deals with who is allowed in or not. That leaves the information itself still unprotected.

I just offer, you know, earlier, in the earlier panel, the question on SB 1386 came up. I share with you, that's probably been one of the more successful legislations in terms of focus because it drove focus on information and how do you protect information. It is a given people are going to get in. The question is, what access to what information do they have when they get in?

If all you are doing is playing defense on the perimeter and trying to keep people out, you are never going to win. You have to offensively protect and encrypt the information on the inside. And the threat in California of class action suit. Every corporate executive understands that, especially in California. So I just offer that identity theft, you can't be stuck on just the identity authentication, it is the information that must ultimately be protected. And anything that I have seen that's been announced up to this point, even yesterday with the ISP, only deals with half the equation.

Mr. PUTNAM. Well, I would like to give this panel the same opportunity that the first panel had, and we will begin with you, Ms. Westby, of giving any closing remarks that you think are important for the subcommittee to have on the record, answering any question you wish you had been asked or giving us any other thoughts.

Ms. WESTBY. Well, I would just leave you with the thought that there are some black holes that need to be addressed beyond technology gaps. One is in the legal framework. There is absolutely no legal framework or rules of law for how nation states will respond to cyber attacks. There is no capability for allied countries to work together to have some sort of allied response.

In defense circles cyber defense is not a category. A defense category is still land, sea and air, and we see cyber as footnotes in presentations. It is also not an integrated response capability. And we have to think beyond, when we are looking at terrorist attacks and information warfare and the potential attacks from other countries, we have to look beyond our legal framework and think about how we can respond in a situation that would involve nation state activity or require coordinated action by other nation states.

Mr. PUTNAM. Thank you.

Mr. Conner.

Mr. CONNER. Mr. Chairman, I want to thank you for your diligence, support of these issues, and your forceful viewing of the hearing on these issues. I would just ask that the task force report on framework—I think this specific subcommittee that did such good work on GISRA and FISMA and putting the report cards out needs to go to the framework of assessment that we are asking private industry to do.

I think part of the problem with the report card piece is it's a different model than what private industries are doing. So there's a gap between the two, and I think you would find you would make much more progress on a benchmark and measurements by using the [ISO] 17/7/99 standard that we consulted with FISMA on to hold the departments and agencies accountable and give them a reference for it, for the private industries they deal with, whether it's DOE with utilities or whether it's Commerce with banks or Treasury with banks.

So I would just offer that as a final comment.

Mr. PUTNAM. Thank you, Dr. Hancock.

Mr. HANCOCK. Mr. Chairman, thank you very much for today and also for your continued leadership in the area of cyber security. One of the things that I think are important to realize with all of this is that we have a problem with corporate governance. I think that's pretty much a given. I think the secondary problem that we have also at the same time is that we have to realize that as we continue to deploy technology we continue to make the networks larger and more complex, and with complexity comes the difficulty of trying to secure it. And we are going to find in a very short amount of time that the size of the Internet will double or triple, and the reason we will do that is because of handsets and because of PDAs and because of other types of portable devices that will become enabled or Internet capable.

We will also simultaneously find the technology that is invisible to us now, such as a refrigerator, will become an important ma-

chine on the network. We know that some vendors are working right now with appliance manufacturers to go back and provide an Internet connectivity with different types of appliances. So someone could turn your refrigerator off from a remote location if they desired or hack it.

The result is that I think what we see is extortive attempts by people now will change. I think that what we will see is identity theft will change, where you will steal an entire city block's worth of IP addresses and sell them off to someone else. I think we are going to see the whole framework of what is an identity theft and what kind of crime could be committed with that change quite radically over the next couple of years.

So I think there is a serious sense of urgency in terms of how do you deal with the identity of both individuals, applications and technology devices, so that we can probably go back over—not just trace these back, but secure them and put them in the proper technologies to make that happen.

Mr. PUTNAM. And, Mr. Schmidt.

Mr. SCHMIDT. Mr. Chairman, I also would like to thank you once again, not only for your leadership, continued leadership in this area, but also for Bob Dix, who as I jokingly told a friend of mine one time as I was driving out of D.C. after I retired, looking back in a rear window, at least Bob is there to keep this fight going. I thank you for that.

Just a couple of quick comments, one relative to the private sector and the government now. We have seen over the past few years the changing of the guard, if you would, when it comes to cyber security within corporations. Executives such as, you know, Mr. Hancock and myself are now outside of the IT organization. We have a special focus on cyber security, no longer just an IT function, which I think is very important, because it is more than just the technology.

Looking at the government side, I think there probably should be some good reviews on how the government functions in that regard. How closely, you know, are we still putting security folks in the IT organization, working for CIOs and somewhat handicap them in somewhat former fashions.

The other portion of it—and both the Secret Service and FBI—we talked about information sharing. I constantly get calls from people because of my law enforcement. background asking me, well, who do I call in the city? Do I call the Secret Service, do I call the FBI? Is it the Electronic Crimes Task Force, the Cyber Crimes Squad? And the answer is not whoever gives you the best service. There should be a much more formal form of consolidation. If we have a cyber crime squad with the FBI, an electronic crimes in the same city, they should be part of a joint task force. And that would help solve a lot of the sharing information issue, plus a lot of the confusion in the private sector on who to call.

And last, as I mentioned, I thank you for asking me that question about the two-factor authentication. We are poised within the government to do something about the stronger authentication piece, OMB's office. I think we can look at that from a two-factor perspective, provide some perspective not only for government employees, but also for the private sector as well, be able to do your

health care, you know a litany of things that could be done that could make two-factor authentication the normal way of doing business as opposed to what we have seen up to now. But thank you once again.

Mr. PUTNAM. Thank you.

I want to thank all of our witnesses for their participation today. Your testimony is further evidence that it is so important for us to take immediate steps to improve our cyber security throughout the Nation. In the event there may be additional questions we did not have time for today, the record will remain open for 2 weeks for submitted questions and answers. We thank you all for your hard work and look forward to continued progress for the remainder of this year and in the next Congress.

The subcommittee stands adjourned.

[Whereupon, at 4:15 p.m., the subcommittee was adjourned.]