AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBERSECURITY: THREATS TO THE FINANCIAL SECTOR

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 14, 2011

Printed for the use of the Committee on Financial Services

Serial No. 112–60

U.S. GOVERNMENT PRINTING OFFICE

72–601 PDF WASHINGTON : 2012

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

SPENCER BACHUS, Alabama, *Chairman*

JEB HENSARLING, Texas, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JUDY BIGGERT, Illinois
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
PATRICK T. McHENRY, North Carolina
JOHN CAMPBELL, California
MICHELE BACHMANN, Minnesota
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
NAN A. S. HAYWORTH, New York
JAMES B. RENACCI, Ohio
ROBERT HURT, Virginia
ROBERT J. DOLD, Illinois
DAVID SCHWEIKERT, Arizona
MICHAEL G. GRIMM, New York
FRANCISCO "QUICO" CANSECO, Texas
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee

BARNEY FRANK, Massachusetts, *Ranking Member*
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN McCARTHY, New York
JOE BACA, California
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
ANDRÉ CARSON, Indiana
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
JOHN C. CARNEY, JR., Delaware

LARRY C. LAVENDER, *Chief of Staff*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SHELLEY MOORE CAPITO, West Virginia, *Chairman*

JAMES B. RENACCI, Ohio, *Vice Chairman*
EDWARD R. ROYCE, California
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JEB HENSARLING, Texas
PATRICK T. MCHENRY, North Carolina
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
FRANCISCO "QUICO" CANSECO, Texas
MICHAEL G. GRIMM, New York
STEPHEN LEE FINCHER, Tennessee

CAROLYN B. MALONEY, New York, *Ranking Member*
LUIS V. GUTIERREZ, Illinois
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
RUBÉN HINOJOSA, Texas
CAROLYN MCCARTHY, New York
JOE BACA, California
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
NYDIA M. VELÁZQUEZ, New York
GREGORY W. MEEKS, New York
STEPHEN F. LYNCH, Massachusetts
JOHN C. CARNEY, JR., Delaware

CONTENTS

	Page
Hearing held on:	
September 14, 2011	1
Appendix:	
September 14, 2011	53

WITNESSES

THURSDAY, SEPTEMBER 14, 2011

Garcia, Greg, Partnership Executive for Cybersecurity and Identity Management, Bank of America	41
Nelson, William B., President and Chief Executive Officer, the Financial Services Information Sharing & Analysis Center (FS–ISAC)	34
Rotenberg, Marc, Executive Director, the Electronic Privacy Information Center (EPIC)	45
Sartin, A. Bryan, Director, Investigative Response, Verizon	36
Schaffer, Greg, Acting Deputy Under Secretary, U.S. Department of Homeland Security	10
Shannon, Gregory E., Chief Scientist, Carnegie Mellon University's Software Engineering Institute CERT Program	43
Smith, A.T., Assistant Director, United States Secret Service	7
Snow, Gordon M., Assistant Director, Cyber Division, Federal Bureau of Investigation	8
Tillett, Brian, Chief Security Strategist, Public Sector Group, Symantec	38

APPENDIX

Prepared statements:	
Garcia, Greg	54
Nelson, William B.	64
Rotenberg, Marc	88
Sartin, A. Bryan	101
Schaffer, Greg	111
Shannon, Gregory E.	118
Smith, A.T.	131
Snow, Gordon M.	137
Tillett, Brian	149

CYBERSECURITY: THREATS TO THE FINANCIAL SECTOR

Thursday, September 14, 2011

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:01 a.m., in room 2128, Rayburn House Office Building, Hon. Shelley Moore Capito [chairwoman of the subcommittee] presiding.

Members present: Representatives Capito, Renacci, McHenry, Pearce, Luetkemeyer, Duffy, Canseco, Grimm, Fincher; Maloney, Watt, Baca, Scott, and Carney.

Ex officio present: Representative Bachus.

Also present: Representative Al Green of Texas.

Chairwoman CAPITO. This hearing will come to order.

This will be our first hearing in the Financial Institutions Subcommittee since the August recess. I would like to remind Members to try to abide by the 5-minute rule when questioning witnesses so all Members will have sufficient time to ask questions. I am sure we will have more Members coming in as the hearing goes on.

Today's hearing will provide members of this subcommittee the opportunity to better understand the challenges financial institutions and their customers face from cyber threats. This year alone, there have been numerous security breaches and attacks on private companies, Federal agencies, and financial institutions. Actually, I think I might include myself in one of those; I think my card got caught up in one of these. Reports estimate that more than $1 trillion is lost annually to cyber attacks and that, on average, a security breach costs a small business approximately $7 million.

These threats are especially acute and worrisome in the financial services industry. In June of this year, Citigroup reported that sensitive account information for 200,000 customers had been compromised by hackers. Statistics show that most of these attacks originate in Eastern European countries that were once part of the Soviet Union. Unfortunately, most of these nations do not regard the actions of the hackers to be a crime so it is very difficult to bring these criminals to justice.

The technological advances that provide hackers with the ability to carry out these attacks also make it very difficult to track the actions of the hackers. In order to effectively combat these hackers, it is critical for financial institutions to share information with other institutions as well as Federal law enforcement agencies.

The Administration and Congress are actively working together on ways to better protect our Nation's businesses and citizens from these attacks, and today's hearing is just one component of this work.

I look forward to hearing from both witness panels this morning. Their testimony and candid conversation will provide Members with a better understanding of this very complex issue.

I am especially interested to hear from our witnesses about the creation of the Office of Financial Research, as has been called for by the Dodd-Frank Act. I have serious reservations about the creation of this new bureaucracy, and I am most concerned with the potential for new cyber threats surrounding the information the Office of Financial Research would be compiling. By compiling sensitive financial information into one Federal agency, are we just making it easier for hackers to attack us? Certainly, that is a question to ask today.

I would like to also say that I am disappointed that the OCC was unable to provide a witness for us here. As the primary supervisory body for many of our Nation's largest financial institutions, their participation is very critical. I hope and I am sure they recognize the role that they play in this conversation and will become an active participant.

I would like to recognize the ranking minority member, the gentlelady from New York, Mrs. Maloney, for the purpose of making an opening statement.

Mrs. MALONEY. Thank you very much, Madam Chairwoman.

And welcome to our witnesses today.

This is an incredibly important issue and an incredibly important challenge before our Nation. The security of our financial system is so important, especially in this digital age where consumers have unprecedented access to financial information, online banking, and trading platforms. They need to know that their personal information is protected and that the systems they access are being protected from large-scale hacking operations.

Like the chairwoman, I also have had my identity stolen, so this is a challenge that we face in our personal lives, as do many of our constituents. Not only is it a threat to our financial institutions, where I understand roughly 22 percent of the hacking is taking place in financial institutions, but it is also our military complexes, our government—every area that we have sensitive information and our intellectual property. So it is critical in all of these areas to protect our information.

I am very pleased that we have impressive panels of witnesses today to discuss the threats to the financial services sector. Threats are growing more real as cyber terrorists become more sophisticated, but our response to these threats has also evolved and grown. And I am hopeful that we are better at it than they are and that we are better at protecting our people than they are.

I will just say, spying has always been part of our lives on this planet. Usually, people got into some costume and hid their identity and came in and tried to gain information, but now one just sits at a computer someplace and can access information, and it is a huge threat to our institutions and to our government.

I would like to hear today how we are cooperating with our international allies who also face this challenge. Are we sharing information? Are we working together? And are we working together between the financial private sector and our government? I know there is proprietary information in the private sector; I know that there is classified information on the government area. But we need to sit down and, in an organized way, work to share this information so that we are stronger in fighting and working together for cybersecurity.

There is one thing we know: Every entity that uses a digital framework or platform is vulnerable. There is no such thing as a completely secure network. And the cost to secure these systems is extremely high, both in terms of protecting against hacking incidents and combating them when they happen.

President Obama has stated that the cyber threat, "is one of the most serious economic and national security challenges we face as a Nation" and that America's economic prosperity in the 21st Century will depend on cybersecurity. I would also say that our national security depends on cybersecurity.

Just this month, the Department of Homeland Security issued a bulletin warning that the hacking collective known as "Anonymous" was planning to target financial services companies and their employees who are "ideologically dissatisfied and sympathetic" to their cause, to give them information and access. Although this group has not launched a wide-scale attack, we know they are attempting to increase their level of sophistication.

This hearing today is an informational one, as we attempt to gather intelligence about the threats to cybersecurity, law enforcement's response, and the impact a cyber attack could have on the financial sector and consumers. But there are a number of legislative proposals already before this Congress, mainly before the Commerce Committee, and they are out there to address the data security and cyber threats. And the Administration has put forward a broad proposal aimed at cybersecurity broadly, not just in the financial sector. The goal is twofold: improve our resilience to cyber incidents; and reduce the cyber threat.

In this hearing, I hope we can better educate ourselves about specific threats in the financial sector and whether there are things that can and should be done to specifically protect financial institutions from cyber threats and to protect the consumers who access financial institutions online. I believe that in a deeply divided Congress, this is one area where we can come together and work with great determination to give the resources and come up with the answers to protect our industries and our individuals.

Since it is the week after 9/11, I just want to share with you that when we worked to create the 9/11 Commission that came forward with the report that outlined 51 recommendations of how to make this Nation safer, their number one recommendation was the need to reform our intelligence system, that our best defense against another terrorist attack was better intelligence. And we have brought together our FBI, our CIA, 17 different intelligence agencies to work together under one Director, sharing information down to the local level with New York City and other cities where we have an anti-terrorism task force. And I believe that this sharing of infor-

mation is one of the reasons that we were able to thwart 12 different attempts, just in the case of New York, to hurt us since 9/11.

I hope we have that same type of sharing and coming together between all of the agencies to combat this very, very serious threat to our national security and to our economic security and to our individual privacy. And I look forward to working with the chairwoman and everyone else on both sides of the aisle to make our country more effective, more secure, and a leader in cybersecurity and protecting our information.

One of the things that we have in this country is the talent of our individuals, our intellectual property. We have to protect that. And I look forward to hearing from the public sector and the private sector, whom I hope are working together in sharing this information, on how you are moving forward to help our great country.

I thank you for your work. I thank you for this hearing. And I yield back.

Chairwoman CAPITO. Thank you.

I would like to recognize the chairman of the full Financial Services Committee, Mr. Bachus, for 3 minutes.

Chairman BACHUS. I thank the chairwoman.

The Financial Services Committee is presented with many important, complex issues and challenges: financial regulation; the health of our economy; the Nation's housing policy; and increasing exports, to name just a few. All of these affect us daily. Another issue that is maybe not talked about as much is cybersecurity, which affects each and every one of us and the companies we deal with every day, whether we realize it or not.

And each of us is dependent on good cybersecurity. Chances are that everyone in this room knows someone who has been the victim of a hacker or has had their identity stolen or their credit cards used for purposes they did not approve or even know about. I have had that happen to me, personally. Because of good cybersecurity by one of our banks, about 2 years ago I was called and told that they had stopped my credit card because they felt there were unauthorized purchases, and, in fact, there were. So they were right on top of it.

The financial services industry, actually, has led the Nation and has really been, I think, at the forefront of developing ways to enhance cybersecurity, and that is because they have been a huge target for cyber crime. The International Monetary Fund and Citigroup, just this last month were targets of sophisticated computer networks offshore trying to crack their systems. Even the Central Intelligence Agency has been a target, and the U.S. Senate recently. So it is just amazing.

At the same time that we are meeting this challenge, government budget cuts have resulted in fewer resources being available to not only our Federal but State and local law enforcement agencies in combating cyber crime. One critical thing is training personnel to deal with it.

And I want to close by commending one of our witnesses, A.T. Smith, and the Secret Service. One of the most outstanding resources that the Secret Service has developed is the National Com-

puter Forensic Institute. We actually had a hearing there in June where we heard from State and local law enforcement officers from all over the country, prosecutors and judges who had been trained there, and as a result of their training, successfully prosecuted cybersecurity cases. In fact, in two recent very high-profile cases, people who were trained at that center actually were forensic witnesses who helped convict individuals.

So I want to say to you and the Secret Service, Director Smith, thank you. Thank you very much for a job well done.

And I would commend anyone to visit that center. Sometimes, we criticize the efforts of our government or the agencies, but if you want to see a success story, that is one place to go.

Thank you.

Chairwoman CAPITO. Thank you, Mr. Chairman.

I would like to recognize Mr. Scott for 3 minutes for the purpose of an opening statement.

Mr. SCOTT. Thank you very much, distinguished chairwoman.

This is an important and very timely hearing. Just 3 days ago, we all recognized the 10th anniversary of the September 11th terrorist attacks on the United States. And along with remembering the victims of that day and the survivors of that day, we have reflected upon what has truly changed and what has continued to evolve so much over the last 10 years. In the past 10 years, in terms of national security and the ability to predict future threats to our country, we have certainly improved. We have been watchful; we have not let our guard down.

This concern has become increasingly relevant as we become more increasingly dependent upon digital devices and methods of communications in general. And as our society becomes more reliant on technology, security experts have brought to light potential vulnerabilities in our technological infrastructure. As many of you may know, the computer networks of our CIA have been breached. The computer networks of the Department of Defense have been breached. And even Federal Reserve Chairman Ben Bernanke—his computers have been hacked and breached.

That is why this is so important. And it is so good to have our key national security and intelligence experts here with us today, and especially in the law enforcement area.

I think it is particularly important that we address about two or three major questions that I certainly have a great interest in. For example, do Federal law enforcement agencies share information about cyber attacks that are experienced by one financial company, or one company, to help other companies to protect their networks? And how can information-sharing be improved between government agencies responsible for cybersecurity and the critical infrastructure of the financial sector? And then, how does the Federal Government compare to what the private sector is doing?

This must be a shared experience, and I am hopeful that Congress will address these threats to cybersecurity appropriately and effectively by means of legislation and that we do it quickly. A number of proposals have been discussed already, namely measures that would strengthen the law enforcement of cyber crimes or provide the Department of Homeland Security with some oversight of Federal IT and critical infrastructure security. Whether such

changes are made piecemeal or as part of a comprehensive bill, we must address these weaknesses in our digital infrastructure right away, quickly, immediately, with all deliberate speed.

Thank you, Madam Chairwoman.

Chairwoman CAPITO. Thank you.

I would like to recognize Mr. Canseco for 1 minute for an opening statement.

Mr. CANSECO. Thank you, Madam Chairwoman, and thank you for holding this very important hearing.

As we will hear from our witnesses today, one of the greatest continuing threats to our country are cyber criminals who target our government, financial institutions, and private American citizens. These attacks threaten both our national security and the stability of our financial systems.

I represent a large portion of San Antonio, Texas, a city which has earned the moniker of "Cyber City, USA" for the numerous collaborative efforts that take place there between industry, military, and academia to deter cyber crime.

While I applaud the efforts by those in San Antonio and from agencies such as the Secret Service in preventing a number of attacks, we must recognize this is an ongoing and evolving threat that requires a great amount of vigilance to combat. And I look forward to hearing from our witnesses today on this important matter.

I yield back.

Chairwoman CAPITO. Thank you.

And our final opening statement, Mr. Grimm from New York, for 1 minute.

Mr. GRIMM. Thank you, Madam Chairwoman. And thank you for calling a hearing on cyber crime and the threat it poses to our financial system.

As a former FBI agent, I am well aware of the threat cyber crime poses to individuals, institutions, and, most importantly, our national security. It is estimated that each year, cyber crime costs the United States $114 billion, with $37 billion of that coming from identity theft alone. This is a cost that is ultimately borne by every U.S. citizen in one form or another.

While many people assume the threat from cyber crime is financial, there has been a growing risk that hostile governments can use emerging cyber warfare techniques to steal vital secrets from the United States and weaken our position in the world. Therefore, I am very interested in hearing what our panelists see as the latest threats that are emerging in this field and what we can do here in Congress to assist in staying one step ahead of those who wish to harm both financial institutions and our national security.

Thank you, and I yield back.

Chairwoman CAPITO. Thank you.

That concludes our opening statements.

I would like to welcome the first panel for the purpose of giving a 5-minute opening statement. We have your written statements submitted for the record.

We will start with Mr. A.T. Smith, who is the Assistant Director of the United States Secret Service.

Welcome, Mr. Smith.

STATEMENT OF A.T. SMITH, ASSISTANT DIRECTOR, UNITED STATES SECRET SERVICE

Mr. SMITH. Thank you. And good morning, Chairwoman Capito and Ranking Member Maloney as well as the distinguished members of the subcommittee. Thank you for the opportunity to participate in this morning's hearing.

One of the significant challenges in analyzing threats that cyber criminals pose to the financial sector lies in the diversity of the online criminal community. For example, criminals may choose to come together around a particular set of Internet-based chat rooms or Web-based carding forums. Diversity is also reflected in the group's interests and aims. However, there is always one common goal among them: financial gain.

Two of the hallmarks that distinguish effective online criminal groups are organizational structure and access to well-developed criminal infrastructure. One of the trends in online criminality first began to merge approximately a decade ago. In the early days, online forums were established by hacking groups or by groups of carders. Today, many of these forums have a strong representation of members from the Eastern Europe theater, although membership in these groups often spans the globe.

Some of these online forums developed into marketplaces for criminal goods and services. By 2004, forums such as DumpsMarket, CarderPortal, Shadowcrew, and CarderPlanet were already well-developed criminal marketplaces. In reality, these sites serve as a business platform for a fusion of criminal communities which provide reliable criminal services to all members.

In collaboration with Verizon on the "2011 Data Breach Investigations Report," the Secret Service has worked to identify emerging threats, educate Internet users, and evaluate new technologies that work to prevent and to mitigate attacks against critical computer networks. The results show that two noticeable trends in cyber crime involve the ongoing targeting of point-of-sale terminals as well as the compromise of online financial accounts, often through malware.

Compared to recent history, it appears that while more data breaches occurred in 2010, the amount of compromised data decreased due to the size of those compromised databases. This change demonstrates the willingness of the criminal groups to go after the smaller, easier targets. In light of recent arrests and prosecutions following intrusions into the financial services firms, criminals may now be weighing the reward versus the risk.

There has been a noticeable increase in account takeovers that result in fraudulent transfers from the victim's account to an account under the control of the perpetrator. This increase can be directly tied to the continued rise of malware variants created to capture log-in credentials and financial Web sites. The Secret Service and the financial services community are working together to combat this growing trend. The FS-ISAC has teamed up with the Secret Service, the Department of the Treasury, the Department of Justice, and many other agencies to create the Account Takeover Task Force, which focuses on prevention, detection, and response to account takeovers.

The Secret Service continues to combat these crimes by adapting our investigative methodologies. Our success is due, in part, to effective collaboration that we have established with the private sector, the law enforcement community, and academia, and our 31 electronic crimes task forces. To date, the Secret Service has currently over 1,400 agents, trained in various levels of computer forensics, serving throughout our 142 domestic and 24 international offices. In fact, we value this training so highly that the basic level is now incorporated into part of the curriculum for all new agents.

In partnership with DHS, the Secret Service has established the National Computer Forensics Institute that Chairman Bachus mentioned a moment ago, and with NPPD to provide a national standard of training for a variety of electronic crimes investigations.

In collaboration with S&T, the Secret Service, the CERT Insider Threat Center, and the Department of the Treasury are all working to update the "Insider Threat Study." This study was the first of its kind, combining both psychologists from the Secret Service and technical experts from CERT to examine insider cases both from a behavioral and a technical perspective. The new study will focus solely on cases that occurred in the banking and finance sector and will be released later this year.

Madam Chairwoman, Ranking Member Maloney, and distinguished members of the subcommittee, the Secret Service is committed to our mission of safeguarding the Nation's financial infrastructure and will continue to aggressively investigate cyber and computer-related crimes to protect the American consumer and our institutions from harm.

This concludes my prepared statement. Thank you again for the opportunity to have the Secret Service at this hearing.

[The prepared statement of Assistant Director Smith can be found on page 131 of the appendix.]

Chairwoman CAPITO. Thank you, Mr. Smith.

Our second witness is Mr. Gordon Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation.

Welcome.

STATEMENT OF GORDON M. SNOW, ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. SNOW. Good morning, Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee. I am pleased to appear before you today to discuss cyber threats against the financial sector and how the FBI is working to protect businesses and American consumers.

As you know, industries continue to adopt Internet-based commerce systems while cyber criminals continue to advance their organization, professionalism, and sophistication. Do-it-yourself cyber crime toolkits have lowered entry barriers for new cyber criminals, making it easy to exploit systems and steal information to be used for financial gain.

Criminal activity is increasingly taking root in countries with emerging broadband infrastructure, making it even more difficult to determine attribution and prosecute the criminals. Malicious

code is more rampant than ever, and average computer users continue to have difficulties installing the security patches that would prevent and protect their systems.

For businesses and financial institutions, the implications are significant. There is a critical need for a major change in the way we think about cybersecurity and protecting our systems against cyber crime. Cybersecurity can no longer be just an afterthought. It must become part of the financial sector's intelligence, planning, and commerce strategy.

The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized, automated clearinghouse wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million.

In 2010, the village of Summit, a town of 10,000 citizens outside of Chicago, was the victim of a cyber intrusion resulting in unauthorized ACH transfers totaling $100,000. When an authorized individual logged in to the town's bank account, the individual was redirected to a site alerting her the bank's Web site was experiencing technical difficulties. During this redirection, the criminal used the victim's valid credentials to initiate transactions. The town was able to recover only $30,000 from these transfers.

Cyber criminals are also targeting the networks of large payment processors. In November 2008, a U.S. payment processor discovered that hackers had breached the company's network and compromised the personal data of over 1½ million customers. Approximately 1 million Social Security numbers were also exposed. The criminals used the stolen data to create counterfeit debit cards and withdrew more than $9 million from ATMs worldwide.

Securities and brokerage firms are also at risk of exploitation. In February 2011, the parent company of NASDAQ confirmed that they had been the victim of a security breach in the "Director's Desk" Web application, a system that was not directly linked to their trading platforms but was used by senior executives and directors to share sensitive information.

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the Administration, we are devoting significant resources to this threat. Our partnerships with industry, academia, and across all of government have led to a dramatic improvement in our ability to combat the threat. With cyber squads in each of our 56 field offices and more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners, we have increased the capabilities of our employees by selectively seeking candidates with technical skills and continually updating our cyber training.

The FBI is also adapting to the ever-evolving technology used by cyber criminals. Intelligence drives operations in the FBI, and the Bureau is working in creative ways with all our partners to address the cybersecurity threat. We currently have FBI agents embedded full-time in foreign police agencies to assist with cyber investigations. These cyber personnel have identified cyber organized

crime groups targeting U.S. interests and have supported other FBI efforts.

The FBI has worked with a number of regulatory agencies to determine the scope of the financial cyber crime threat, develop mitigation strategies, and provide public service announcements where appropriate. The FBI partners with criminal investigators from the United States Secret Service and other law enforcement agencies, along with members of industry government entities such as the National Electronic Payments Association and the Financial Industry Regulatory Authority.

The FBI has been able to mitigate a number of fraud matters by sharing identified threat data amongst financial-sector partners. A good example of this cooperation is the FBI's identification of a bank fraud trend in which U.S. banks were unaware that they were being defrauded by businesses in another country. As a result of the FBI intelligence analysis, a joint FBI/Financial Services-Information Sharing and Analysis Center document was drafted and sent to the FS-ISAC's membership, alerting them of these crimes and providing recommendations on how to protect themselves from falling victim to the same scheme.

Another recent success was the combined efforts of the FBI and the Department of Justice and industry subject matter expects to take down the Coreflood botnet. This botnet infected user computers and stole banking credentials and other sensitive information. In this instance, government and private industry worked together to provide an innovative response to a cyber threat. Not only was the botnet shut down through a temporary restraining order, the government was authorized to respond to signals sent from infected computers in the United States in order to stop the Coreflood software from running. This prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the United States.

We at the FBI are faced with an enormous task fighting cyber crime. We are gaining traction, but we need the full support of every stakeholder. A successful fight against cyber crime will require a combination of people, processes, and technologies across multiple entities. We look forward to working with the subcommittee and Congress as a whole to determine a successful course and outcome.

Thank you.

[The prepared statement of Assistant Director Snow can be found on page 137 of the appendix.]

Chairwoman CAPITO. Thank you.

Our final witness on this panel is Mr. Greg Schaffer, Acting Deputy Under Secretary, Department of Homeland Security.

Welcome, Mr. Schaffer.

STATEMENT OF GREG SCHAFFER, ACTING DEPUTY UNDER SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SCHAFFER. Thank you, Madam Chairwoman, and thank you, Vice Chairman Renacci and Ranking Member Maloney, for having me here to testify about DHS's efforts to reduce risk from cybersecurity issues to the banking and finance sector.

It is really quite hard to identify a security issue today that is more pressing than cybersecurity. Indeed, this is an area that raises issues of national security, homeland security, and economic security for our country.

The reality is that we are increasingly under attack in a dangerous cyber environment. The attacks are more targeted, more sophisticated, and more serious than they have been in the past. Our adversaries are stealing sensitive information, both from government and from industry, and they are taking away our comparative economic advantage as they do so, as well as jeopardizing individual privacy.

More disturbing, as more and more of our infrastructure is attached to these networks, we know that our adversaries are capable of targeting and impacting the elements of critical infrastructure that underpin our financial systems and other critical infrastructure. Major financial institutions and those resources that they depend on, like communications and the electric grid, are all subject to attack. And, indeed, this is not conjecture. This is happening on a daily basis, with hackers probing and attempting to impact critical infrastructure entities. Moreover, because our financial institutions are critical to our Nation's economic security and handle large sums of money, they are, needless to say, targeted for many of these attacks.

In response to these growing and persistent issues, the Department of Homeland Security, along with our Federal partners, are working collaboratively with the financial institutions to assist in defending and securing our Nation's most essential networks. This public-private partnership is extremely important to our success in protecting our infrastructure. No single technology, no single entity in government or in industry can solve this problem alone. This is truly a shared responsibility.

The National Protection and Programs Directorate, or NPPD, within DHS has several cybersecurity roles. First, we protect the Federal Executive Branch civilian networks, or the dot-gov space. Second, in partnership with our private-sector partners and others within government, we lead the protection of critical infrastructure, working with industry to provide technical expertise, to broaden risk-assessment capability, to develop mitigation strategies, incident response capabilities, and generally reduce risk. We are responsible for coordinating national incident response capabilities, working with law enforcement agencies, the intelligence community, the defense community, and Homeland Security resources across the Nation. And, generally, we are tasked with raising awareness of cybersecurity issues across-the-board.

Financial sector initiatives that we are working today are diverse and many. Our relationship with critical infrastructure stakeholders has matured over the course of the last several years, so we are not just thinking about information-sharing for the purpose of information-sharing, but operational risk reduction through information that is really actionable by those entities that receive it.

For example, we are now working with the private sector, literally living on the watch floor at the National Cybersecurity and Communications Integration Center. The financial services sector, as well as other sectors, are placing resources on the watch floor

so that we are breathing the same air and learning about incidents as they happen and able to respond to them together as a team. The financial sector's presence really enhances the analysis, warning, and response capabilities associated with critical information systems.

We are also working with the financial services information-sharing pilot, the FS-ISAC, the Financial Services Information Sharing & Analysis Center, to share information between DOD, DHS, and the financial services sector. Government has provided over 2,800 informational products to the financial services sector and received over 394 submissions over the course of the pilot. And, indeed, that pilot has shown us, and we have learned, that both government and industry have information of value to each other that we would not have if we were not working in collaboration. Based on the success of the pilot thus far, we plan to extend this to several other industry sectors over the course of the coming year.

We have a resiliency review pilot ongoing, as well. We are working in two phases to work with the sector in order to do assessments of their cybersecurity resiliency as well as looking for malicious actors on their networks. We provide a range of technical assistance to actors when they request it. And, indeed, over the course of the last year, we have provided assistance to several institutions in the financial sector.

I thank you again for the opportunity to provide you with testimony this morning and stand ready to answer your questions. Thank you.

[The prepared statement of Acting Deputy Under Secretary Schaffer can be found on page 111 of the appendix.]

Chairwoman CAPITO. Thank you. Thank you all.

And I will begin the questioning with a question of Mr. Snow.

You mentioned "botnet." Can you explain that to me and what that means for an individual computer user? Because that is where somebody can use my computer to go in and compromise other people's financial data; am I understanding that correctly?

Mr. SNOW. Correct. And the simplistic way to look at it is, it is a network of computers run by a malicious actor that acts autonomously. So your computer could be under the control of another individual to run this bot. The bot herder would be the name of the individual. He would run this bot that could be a series of a million, 2 million computers that are controlled by command-and-control servers, one or many, depending on the size of the network.

And those computers would work on their own. For instance, in the Coreflood botnet, as soon as you open a browsing window or added in personally identifiable information, the key-logger would grab that information. And then, periodically, the way the malware was set up is it would send it to the command-and-control server under the control of the criminal actor, who would use that information for whatever purpose they deemed appropriate—selling it online, using it to profit, and other things.

Chairwoman CAPITO. So when we, as individual computer users, log on and we think we have security-ware on our computer, that may be a myth for some—for most of us, probably?

Mr. SNOW. It may not be a myth if you are paying a subscription. You may actually have your security antivirus there. The myth

portion of it is just that it may not have the signature or be able to identify that bot.

For instance, in the Coreflood botnet, it was almost every 48 hours or 72 hours, there was an update sent to the botnet so that the antivirus signature would be behind the power curve.

Chairwoman CAPITO. Okay.

So that was kind of one of my impressions, just listening to all three of you, is that it is so difficult to stay one step ahead. Because as soon as you change your technique to discover, then they change their technique to be undiscovered. And, obviously, they are very bright computer folks, with bad intentions at the same time.

Mr. SNOW. Correct. And the point that you brought up about the individual is very salient. The individual, even if they are trying to practice good hygiene on the computer, trying to update their software, trying to look for indications that there may be a problem, may never see that. And, in addition, that malware may disable their antivirus.

Chairwoman CAPITO. Let me ask you about—and this is for anybody—mobile payments. We are learning that we are going to be going—and, actually, I saw this at the airport the other day, where, instead of having a physical boarding pass, they used their mobile phone as the boarding pass.

Do you see this as another chance to weaken the security system? Is it going to be harder to control mobile payments, and is that going to open up a whole new world?

Mr. Smith?

Mr. SMITH. Clearly, I am not an expert on that, but what I have learned is that, as you said, as the technology moves forward, that is going to become more in vogue, probably, to be used.

It probably has some negatives. One of the positives might be that if you are using your mobile phone to make an online payment or withdraw from an ATM, the GPS mechanism may actually be able to detect, if you are making that withdrawal in Washington, D.C., that you are, in fact, there, as opposed to trying to make a withdrawal from Paris, France, if you will.

So I think there are probably a lot more technical advantages to it than disadvantages, but, as you said, there will be people out there who will continue to try to breach it in one way or the other.

Chairwoman CAPITO. Would anybody else like to comment on that?

Mr. Schaffer?

Mr. SCHAFFER. Madam Chairwoman, I would simply add that, as we see new technologies come to the fore, the most important thing is that we focus on the security aspects before those go into wide usage. In other words, there are risks associated with all new technologies. If they are implemented in a secure way, they can be made secure and made to function in a way that serves the purpose of the institutions that are bringing them to the fore.

But if we don't focus on that in advance, if we are not paying attention, the more complex the technology, the more opportunities there are for some of these malicious actors to take advantage of them. And so it is critically important that we don't try to bolt security on afterwards when we find out there is a problem, that we think about it as we go to market.

Chairwoman CAPITO. Right. Right.

One of the questions in my mind as I read through your testimony—there are a lot of commissions. And you mentioned, Mr. Schaffer, in your testimony, collaboration with the private sector. Obviously, the FBI and the Secret Service are collaborating.

This is a judgment question on your part. I don't know if this is something you want to get into, but are you satisfied with the information-sharing that is going across different agencies? How can we improve that?

And, obviously, this is an international forum. Does that present challenges to certain agencies? You mentioned that the Secret Service has international offices, but I didn't know jurisdictionally if that is a problem.

Mr. SCHAFFER. Ma'am, I would say that we are in a better place today in terms of information-sharing than we have been in the 15 to 17 years I have been in this space, both in government, where we have broad collaboration and methodologies that are laid down in things like the National Cyber Incident Response Plan that help us to coordinate our activity as these events occur, and in the private sector, the opportunities for people to literally be on the watch floors with us and then have that information shared.

Do we need more information-sharing? I wouldn't say—I would suspect that all of us would say we always need to have this information flowing as aggressively as possible, and there is more that can be done. But we have certainly made a lot of progress.

Mr. SNOW. I agree wholeheartedly with Mr. Schaffer. But I would state that one of the things that I think we are missing here is the timeliness with which the information is shared. We have to go from manual speed to network speed.

If we are talking about a JTTF information exchange, for instance, we have might have a person or individual; we notify those people, and we work that case. In this instance, this threat comes at us in nanoseconds. It keeps on moving. If I wait until the time that I see A.T. or Pablo Martinez or Jeff Irvine to exchange that information, we have probably already lost the battle. We need to be able to figure out how we can do that in realtime.

Chairwoman CAPITO. All right. Thank you.

Mrs. Maloney?

Mrs. MALONEY. Thank you for your testimony.

And since this is our first meeting since 9/11, and we rarely have the Secret Service, the FBI, and Homeland Security before us, I would like to collectively congratulate you and thank you, on behalf of my constituents and New York City and probably the whole country for your excellent work in locating Osama bin Laden. Thank you.

On this we all agree, that cybersecurity is a threat to our economic security. So I would just like to ask you collectively, what keeps you up nights? What are you most concerned about? What do you feel we really have to do to be prepared?

And this is a Financial Services Committee hearing, but are the attacks different for financial institutions or, say, domestic military contractors and the government or the Stock Exchange? Is there something that is unique about financial institutions?

Also, are you collecting where it is coming from? Is it primarily foreign countries, such as Russia, possibly China, India? Where is it coming from? Is it government-sponsored in other countries or is the threat from other competitors against financial institutions or just plain American criminals trying to steal identities?

I was struck with your testimony, Mr. Smith, so I wanted to particularly respond to your statement that there are increasing levels of collaboration among cyber criminals, particularly in the online space. What steps are we taking, collectively, to work with our international law enforcement against these sort of collaborative international efforts to hack into the information systems of America?

Again, thank you for your work. And what can Congress do to help you? That is it.

Mr. SMITH. Thank you, ma'am.

With regard to the description that you gave, I would say that it is all of those things that you outlined. There are definitely malicious actors out there. There are groups who do this sort of thing. And, as I said in the testimony earlier, we see quite a bit of that activity in the European theater.

What we have done in the Secret Service, and just to follow-up on what Mr. Snow said a moment ago, we are sharing information better than we ever have. Whether it is through the NCIJTF or the FS-ISACs or just collaborating on best practices, if you will, we are better at that than I believe we ever have been.

In terms of the Secret Service and what we have tried to do to fight this issue that we see largely in that theater that I described, we use our liaison efforts in our foreign offices, 24 of them around the world, to make sure that we are in constant touch with the law enforcement entities in those countries. We have recently opened a small Secret Service office in Tallinn, Estonia, which, again, for a number of years has been a hotbed of this type of cyber crime. We have also tried to expand our footprint in other places; we recently have just opened an office in Beijing, China.

So, to address all of those kinds of things that you described, whether it is individuals or organized criminal groups, we have moved in those directions.

Mrs. MALONEY. But when you said Eastern European, are they operating out of Europe? Are they operating out of America?

Mr. SMITH. Probably both. We have had some significant cases where we have arrested people in the Eastern European countries. And, again, that is usually done through the assistance of the host government, the law enforcement entities in those countries. So a little of both, quite frankly.

Mrs. MALONEY. Okay.

And, Mr. Snow, would you like to comment on what keeps you up at night, what are you most concerned about, and what do you feel we should be doing more of?

Mr. SNOW. Currently, what keeps me up at night is my 9-month-old. But the—

Mrs. MALONEY. That is a happy occasion.

Mr. SNOW. The threat that keeps me up the most is just a concern of how we are actually looking at the problem and attacking it.

For instance, if we look at the standards, the industry standards, across networks in all organizations, whether it is government, private sector or public sector, I don't think they are very high. We talk a lot about the advanced persistent threat. It may be persistent because it is still resident in the system, but I don't know that the techniques that we are using, to use a high school analogy, is the varsity team that is coming in. It is the freshman team who is walking in with phishing emails and getting a socially engineered attack that allows the malware to move laterally across the systems.

Mrs. MALONEY. Is the attack different for different institutions, say, a military contractor or the government? Do they use a different system than going after financial information? And how much of it is competitors trying to get information?

Mr. SNOW. It is a great—

Mrs. MALONEY. Or is it just criminal?

Mr. SNOW. Right. It is a great question. And I think if you would have asked me that question about 2 years ago, I would have said there are many variations and different levels of types of information they are looking for. Currently, though, they are so successful, they are looking for all information. So whether it is a clear defense contractor, whether it is a banking institution, whether it is a national security concern or issue, they are looking for the same things, using the same techniques, to pull everything that they can pull off of it.

I would want to ensure that we are moving in a more realtime fashion. I know that we always have privacy and civil libertarian concerns. At the FBI, we take protecting people's civil liberties and their rights and their privacy very seriously. And, at the same time, I look at a system that has been developed to freely share information. It wasn't developed to work on a commerce-type issue or to have people ride on it without any identification. So I would want to have a structure that does two things: one, that offers assurance that those pieces and the parts of the network are protected; and two, that I have some way to look at the identity of somebody taking an action on that system.

Mrs. MALONEY. Great. Thank you.

Chairwoman CAPITO. The gentlelady's time has expired.

Chairman Bachus is recognized for 5 minutes for questions.

Chairman BACHUS. Thank you.

I read your written testimony last night. As many members of this committee may or may not know, we actually have a detailee from the Secret Service. And I hope most of the Members and the general public would simply be overwhelmed with the level of the threat of cybersecurity. There is a great need to educate the public.

And one question I might ask—and you touched on this, all of you—is that these are very sophisticated enterprises that are conducting most of this. Most people kind of have a tendency to think of these as sort of like the Nigerian scheme, where there is some guy sitting in a room in Nigeria, but that is really not the case. That goes on, but this is a much higher, more sophisticated level.

Many of the people who are conducting these have been trained, have master's degrees, have 30 years of experience in the government in another country or working for a technology company in

these countries. And they are well-funded; they are multimillion-dollar organizations. I think you have done an incredible job.

When we talk about funding, that is one thing that worries me. Last year alone, I think there was $7 billion or $8 billion worth of fraud that was prevented. And the amount of information—I know, Mr. Smith, in your testimony, you pointed out that you had to review more information—or 4 times as many terabytes as are in the Library of Congress archives to get this information.

Another collateral benefit is that we solve other type crimes, because the training that goes into this for your agents and your expertise that is developed in this area allows you to—you can apply it in terrorism. You can actually apply it in missing children, some of the training, just across-the-board—child predators.

A number of cases have been solved by training that was received at the National Computer Forensic Institution where local law enforcement went back or judges were able to successfully prosecute people and make the right ruling. Because what you have to successfully do to get a prosecution is you have to be able to successfully extract it from the computer, the information, find it, which is not easy. Then you have to be able to preserve the chain of evidence, and then you have to successfully introduce it in a prosecution. That sometimes has been the problem, that you had the information, but somewhere the chain of evidence was broken, and some sharp criminal defense lawyer was able to take advantage of that.

Mr. Snow, you mentioned Pablo Martinez, who is the Assistant Special Agent in Charge, and then I guess Deputy Assistant Director Jeff Irvine, who I think is in charge of—what is it—34 offices overseas? Somewhere in that neighborhood?

Mr. SMITH. Twenty-four, yes, sir.

Chairman BACHUS. Would you two gentlemen stand up? I want to commend you all for your efforts. And I think probably, each day, the efforts of you and your organizations—and thank you—really keep us all from being ripped off.

And the banks have done a tremendous—the financial institutions are spending millions and millions of dollars in this effort, and the collaboration is so important. And, as I said, the collateral benefit. There is almost no crime today that is committed without the involvement of either a cell phone or a computer or a handheld device. So it is pretty astounding.

My time—I have 11 seconds left, so I just want to say, job well done. And it is an incredibly difficult job.

And I would say to the banks—I know you are on the second panel—I do think it would help if the public and the financial institutions would accept the fact that we may need to go to a protocol of getting into your account with two or three different levels. And I have seen evidence that the financial institutions are doing that. One simple password is becoming pretty archaic now.

Chairwoman CAPITO. Thank you, Mr. Chairman.

Mr. Watt for 5 minutes for questioning.

Mr. WATT. Thank you, Madam Chairwoman.

And let me applaud the chairwoman and ranking member for convening this hearing, and thank these gentlemen for the work that they are doing in this area.

After spending all of the last term of Congress learning about derivatives and CDOs and all of those complex financial matters as chairman of the Domestic Monetary Policy Subcommittee over here, I had an interesting choice at the beginning of this term of Congress and chose to go over and spend most of my time on the Judiciary Committee as the ranking member of the Intellectual Property Subcommittee.

Some of these gentlemen have testified over there about the nature of these problems, because now we are learning about rogue and bogus Web sites, and online piracy, and theft of music and movies, and knock-off drugs and auto parts and military equipment, and just about everything that you can obtain legally can be obtained illegally online, which is all part and parcel of this whole cybersecurity issue.

Chairman Bachus was right, because a lot more theft—we used to think of bank robberies taking place by people walking into a bank with a gun, but all the robberies of banks and accounts are taking place electronically now. Almost nobody walks in with a gun anymore to do that. But the scope of it is mind-boggling, and the technology has made it so easy to steal music and everything else out there, and a lot of control of this is offshore.

So, the magnitude of this problem has made this a national emergency, really an international emergency, that these gentlemen are describing the national component of. But under that there is a commercial component, an industrial component, a banking component that is staggering in its magnitude.

On one aspect of that, we are about to introduce a bill in the Judiciary Committee, a bipartisan bill. One of the reasons I chose to go over to Judiciary at this time, at least the intellectual part of it is more bipartisan than the Financial Services Committee used to be. It is about the only place you can get some bipartisan agreement on something, when you are dealing with some of these issues. So we are attacking the commercial component of it hopefully in this by giving more authority to get jurisdiction over these foreign Web sites, which has been a major problem for the FBI to even get access or jurisdiction over these entities.

I have learned a lot more about this than I ever wanted to know. I didn't know what a "cloud" was until—I thought people were walking around with their heads in the clouds, and now we are storing everything in the cloud. It has been an interesting learning experience for me, just as the last term of Congress was a learning experience for all of us about all of these sophisticated financial products.

I am learning about all the sophisticated ways that people steal and produce bogus products, pirated products. "Knock-offs" is the term I guess we use for them on the street. But there are knock-off drugs, pharmaceuticals. Our military, we haven't even figured out a way to stop our military from buying knock-off, pirated parts for military equipment.

So the problem is massive, and the bottom line is I thank you all for spending some time exposing it in the financial services and the whole cybersecurity area. Thank you.

Chairwoman CAPITO. Thank you, Mr. Watt.

Mr. Renacci for 5 minutes for questioning.

Mr. RENACCI. Thank you, Madam Chairwoman. I want to thank the witnesses for being here today and discussing this topic.

Coming from the private sector and the small business world just recently, as you get up every day, and you worry about making payrolls, and you worry about just keeping your business going, a lot of this doesn't really hit home until you are sitting here listening to it.

I was wondering, from all three of your perspectives, do you believe that private industry and the government agencies are really doing enough to educate the general public and the small businesses and community banks of the safety and security conduct issues that they have to be concerned about with online transactions these days? I would like to hear your thoughts.

Mr. SCHAFFER. Thank you, Congressman.

I do think that there is a tremendous amount of effort going into communicating to the business community. At DHS, we have a number of programs to do that. One which is about to start is National Cybersecurity Awareness Month, the month of October. We will spend a significant amount of time with seniors and others working around the country, and indeed internationally, to talk about cybersecurity broadly to the public.

We have the "Stop, Think, Connect" campaign, which is really designed to speak to individuals about paying more attention to what they are doing when they are clicking through on these links that can cause them to be exposed to some of this malicious software and then become part of a botnet and part of the problem.

There are a variety of things that do need to be done to reach out to small businesses, and both DHS and the Department of Commerce and others have taken some steps to do some of that reaching out to make it clear there are resources like on the US-CERT Web site where you can get information about how to secure your systems and get information about threats and vulnerabilities made available to the public broadly, and there are many places where that information can be obtained.

I do think that this is an issue that we cannot just focus on security professionals. They understand the issue. They are with us. This is an issue that has to be shared with data owners, the folks who are making business decisions about where to invest. The lock on the door, as someone pointed out, the theft is happening through the Internet more than it is happening through breaking into the back storage room, and people need to invest accordingly and risk manage accordingly, and we have to reach those folks and make them understand that shift has occurred, and they need to adjust as well.

Mr. RENACCI. Mr. Smith, particularly from a small business standpoint, do you have any suggestions for small business owners? They don't have the dollars in many cases that the larger institutions have for protection. What are some of the things that a small business owner can do to protect themselves from these security breaches?

Mr. SMITH. You are exactly right, Congressman. You heard from my testimony that some of the smaller businesses and financial institutions have become more of the victim over this past year or so. There are a number of things that they can do, and obviously prob-

ably one of the best things they can do is just consult the FTC's Web site.

But I do want to point out, and I mentioned in my remarks, the Verizon 2011 data breach study that Verizon and the Secret Service, and also from the European theater that we mentioned, the Dutch High Crimes Unit participated in this report this year, and it gives a lot of valuable information about breaches, about hacks, and then also further would probably be a very good tool that small businesses and financial institutions could use in terms of prevention and that sort of thing. It certainly talks about how the hacks occurred and sort of what kind of crimes were perpetrated against them.

Mr. RENACCI. Mr. Schaffer, are you having unique challenges hiring people in regards to cybersecurity?

Mr. SCHAFFER. Yes, sir. We indeed do have some challenges in that regard. The marketplace for deep cybersecurity professionals is extraordinarily competitive. Pay in that space is higher than it is for many other professionals who have an IT or information technology background.

As a consequence, with the Department of Homeland Security trying to hire into a space where even others in government have more hiring flexibility—DOD, for example, has significant authority that DHS does not currently have to bring in those deep technical experts—we would love to have that same kind of capability, and that is part of the legislative proposal that is currently circulating.

Mr. RENACCI. Thank you.

I see I am running out of time. I yield back.

Chairwoman CAPITO. Thank you.

Mr. Scott for 5 minutes.

Mr. SCOTT. Thank you very much.

I was very intrigued by the fact that the CIA, the Department of Defense and our Fed Chairman's computers were hacked. Let me ask you something, because in order to know where we are going, we can learn from experiences that we have gone through. What did we learn from that experience? Who did this? What were they after? What kinds of information did they obtain?

Mr. Schaffer, each of you, if you could. It would be important for us, because I think it is important to know who did this, why they did it, what kind of information did they get, what were they after, and what have we done to correct it?

Mr. SCHAFFER. Congressman, as I think you have heard across the panel today, the number of entities that have been breached and are constantly under attack far exceeds the few that have been mentioned. Literally every department and agency has had attacks against it at various points in time, and those attacks are from a wide array of threat actors that go from individuals to hacktivists or people trying to take political action on the Net, to organized criminal organizations, to nation state actors. It really does run the gambit.

The good news from our perspective in terms of defending these networks is that most of the studies, including the Verizon study that has been referenced that was done with the Secret Service, showed that much of the vulnerability that is being taken advan-

tage of by all of these actors is known and can be fixed by good hygiene and aggressive cybersecurity efforts. We know how to do this. We just need to make sure that our public and private-sector entities are, in fact, executing against those security requirements.

Mr. SCOTT. Do either of you want to comment on that?

Mr. SNOW. Congressman, I would say a couple of things also. One is—and we talk and relate it back to small business—most of the time the people's awareness is only triggered by a loss or an intrusion, and it is the first time that they are actually reaching out for some of the partners or law enforcement or even their peers in the community.

I think we learned after 9/11 that one of the things we need to do is really look at risk, what are your threat times, your vulnerability times, your consequence, and how can we fix those things. How do we table-top those issues? And if you are the IT person or the CEO for the corporation or whatever it happens to be, I know we have to make decisions based on dollars, but we should run even the first run-through of if today you got hacked, what was vulnerable on your networks? Are we really looking to manage and secure systems, or are we looking to manage and secure information? Is your IT person, is the general counsel of that organization, are they good with your IT person's decisions? Is the CEO okay with those decisions? Does anybody understand, as the chairwoman referenced before, that there are proprietary contracts in there that may preclude sharing that information robustly? And how do we go forward taking a look at those issues?

Mr. SCOTT. So we would say, then, that what we have before us is a situation where it is the machinery, it is the system, it is what we have out there, this new technology that we have in and of itself, and that the threats are not necessarily primarily at this point terrorists as much as they are competitors, as much as they are criminal organizations, as much as they are maybe other nations. Is that a fair assessment? From some of our information, we found out that it is not necessarily terrorists who are at the top of the list here in all of this, but it is these other entities.

What I am trying to get at is we have to figure all of this out if we in Congress are going to try to fashion some legislative remedies. We have to get our hands around what it is if we are going to do something significant.

And that leads me to, and I don't have much time, given all of this, what do you recommend when we look at this? It is like a bowl of Jell-O. You get your hand around some of it, and another squeezes out. How do we legislate? What do you recommend that we do legislatively here in Congress to address this extraordinarily difficult and complex issue?

Mr. SNOW. Sir, I will take the question in two parts. One is, where does the threat reside? And honestly, the highest threat is the counterterrorism threat of a terrorist hacker moving into our infrastructure that protects our way of life and our basic necessities and our needs throughout the Nation.

The largest threat right now is the nation state threat that comes in and takes a look at all of our critical research and development, our intellectual property, the things that are coming in lock, stock and barrel, and copying and moving off. In that threat

is included the criminal threat, and I think this Financial Services Committee is focusing in on it correctly. The criminal threat to the economic security of the United States is very critical.

What do we do about it? I think that is an answer for all of us. But one of the things we really need to do is sit down and talk about what are those options we are going to take. How do we engage as a Nation? First, what are the citizens within the Nation willing to accept on how they want to be protected; and second, what are we as a Nation going to do as we respond to the threats we see? Are we appropriately engaged in the domestic intelligence, military, economic, law enforcement model?

I would pass it over to my peers here.

Chairwoman CAPITO. I think the gentleman's time has expired on his questioning.

Mr. Duffy.

Mr. DUFFY. Thank you, Madam Chairwoman, and I appreciate the witnesses coming in for their testimony.

As an individual, is the main threat that comes the individual's way through phishing emails, or are people's computers being hacked on the individual side?

Mr. SMITH. Congressman, it is actually both. We still see a lot of phishing that occurs and people respond to, and, again, a good public awareness campaign is probably as efficient as anything. By the same token, we do see account takeovers and large quantities of personal identification that is actually taken in these kinds of instances that we talk about.

Mr. DUFFY. And on the attacks that are happening, whether they are hacking into computers or they are sending out phishing emails, is it fair to say that a large percentage of the attacks are coming from outside the United States?

Mr. SMITH. Yes, sir, they are. And I believe before you got here, I covered the fact that we have tried to force multiply our efforts, if you will, through our liaison efforts in our foreign offices to make sure that when we encounter criminals in other countries, we have the right liaison effort there, and we can get the right cooperation from the local law enforcement in those countries to try to arrest the people responsible for those things as well.

Mr. DUFFY. And that is where I was going to go with the next question, because if you look at folks who plan and carry out terrorist attacks on our country, we pursue them pretty aggressively, or, as someone mentioned, walking into a bank with a gun and robbing a bank, we also pursue those folks pretty aggressively as well. On one side we are either killing them or capturing them, and bank robbers, we are putting them behind bars for a lengthy period of time.

How successful are we in branching out around the world to get these folks who are actually orchestrating these attacks on our country, because if they pursue several attacks, and we don't apprehend them, they just sit there and attack and attack and attack until they are successful. Are we able to get those folks who are orchestrating the attacks on the country?

Mr. SMITH. We are, and we are very aggressive when it comes to trying to pursue these individuals. Again, a lot of it depends on the country that they may reside in as to the level of cooperation

that we may get. But through, again, our international efforts, we liaison to the nth degree, if you will, with those host countries. And we have tried to do that through another means, and that really affects the public outreach piece, and that is through our Electronic Crimes Task Force. We have 29 domestic task forces that have quarterly meetings that involve both State and local law enforcement, the private sector, particularly the financial sector, as well as academia, to keep us on the cutting edge of what is out there.

But we have also recently organized and started two electronic crimes task forces overseas, one in Rome, Italy, and the other one in London, England. So we are trying to take the model that has worked for us dating all the way back to 1996 in New York City and make that spread not only across the country, but now around the world, and then through those efforts and through that liaison we are able to, we believe, force multiply our efforts and get by on, if you will, from those countries where we actually have to go and investigate these crimes.

Mr. DUFFY. Are we seeing that more of these folks are then congregating in these countries that are less cooperative with their law enforcement agencies?

Mr. SMITH. I really can't give you a statistic for that because they are all over. Again, we talk a lot about Eastern Europe and that area, but there are certainly criminals who do this sort of thing in other parts, in Asia. So I don't think really there is a hard figure for that.

Mr. DUFFY. My time is just about up.

I think one of you mentioned this. It is fair to say that we do have the technology to protect ourselves. Is it just a matter of making sure our financial institutions and our individuals are implementing the procedures and the technology to make sure they have that firewall from these folks?

Mr. SCHAFFER. To be sure, what we have seen statistically is that a significant percentage, a very high percentage of the attacks can be dealt with through good implementation of current technology. That is not to suggest that we can deal with everything in that regard. And there are some sophisticated attacks that current technology is not going to address, and we will need to develop additional capabilities in order to do that.

Unfortunately, today, offense wins in cyber. Defense has to be perfect everywhere; offense only has to be right somewhere. As a consequence, we have a challenge on our hands, and we do need to get to the next level from a technological perspective to be able to get to the point where we change that paradigm.

Mr. DUFFY. And do we have the resources available to pursue those technologies, to make sure that we are being proactive instead of reactive to these attacks?

Mr. SCHAFFER. I think we are definitely being proactive. For example, one of the things that DHS did earlier this year was to publish a paper about what we think needs to happen from an ecosystem perspective to get to the next level, where we have more automation, better interoperability between security solutions, better authentication of people, devices and software. And there are indeed initiatives like the Trusted Internet Connections Initiative,

the name of which just has slipped my mind, that are designed to try to get us to a better place on that authentication issue.

So there are several pushes under way to get those new technologies in place, but it is something that we have to continue to be vigilant about.

Mr. DUFFY. I want to thank you all for your hard work.

I yield back. No more time.

Chairwoman CAPITO. No more time. I would add 'speed," because we have already heard that speed is an issue.

Mr. Baca for 5 minutes.

Mr. BACA. Thank you very much, Madam Chairwoman.

One of the questions that I have, the United States has a separate law imposing data privacy requirements for financial information and for medical information. Do you think it is preferable to have the data protection requirement imposed based on who holds the data, or should it be based on the type of data, regardless of who holds the information? That is for any one of the panelists.

Mr. SNOW. Sir, obviously I wouldn't make the legislative decisions for the Department of Justice or weigh in on it, but I would say that I think it is regardless of who holds the information. As technology and innovation changes so rapidly, I think there would be a desire to offload cost by offloading the information to somebody who may not have that same regulatory requirement. But, once again, that is just a personal opinion of my own.

Mr. BACA. Anybody else want to weigh in on that? Everybody wants to take a pass on it, right?

Okay. Let me ask the next question. To DHS: Can you elaborate on the information-sharing pilot and what lessons have you learned from it, and how do you expect it to inform future actions that you take in this area, which is question number one; and does the financial sector have a unique set of challenges as opposed to other sectors with respect to the cybersecurity; and can you describe some of the unique challenges that you see with respect to the financial sector?

Mr. SCHAFFER. Yes, sir. Thank you for that question.

I think we have learned some lessons from the pilot activity with the Financial Services Information Sharing & Analysis Center. That pilot has shown us a couple of things: first, that each sector has its own technological choices. It has implemented in financial services a set of solutions that are different, for example, from what the defense industrial base has employed, and we need to be able to craft our capabilities at US-CERT as we push out information to be ingested and used and made actionable by the sector. It is going to have to be slightly different for the financial services sector than it was for the DIB, for example.

Second, we have learned that interaction between analysts, the analyst-to-analyst discussions which we have done quite a bit of throughout the pilot, are enormously valuable; that having folks sit down and actually discuss where things are going, and what mitigations are available, and how best to implement those mitigations moves the ball tremendously and allows for greater efficiency and effectiveness on both the government side and the private-sector side.

Third, we have learned that having representatives on the watch floor, as I have mentioned a couple of times, really does enhance the ability to stay up to speed on what both sides are doing and make sure that we are able to, if something is ratcheting up, have good situational awareness from steady state to crisis if indeed something is getting more challenging.

With respect to unique challenges for the financial services sector, I think you have heard these gentlemen speak to it. The fact is the financial services sector is where the money is, and so that sector is targeted in a way that other sectors may not be because there is availability of ready cash. What we are seeing is that intellectual property is being targeted across the entire economy and across all sectors, government and industry, but in terms of direct access to cash, this sector is particularly valued by those who would do us harm. So that targeting puts this sector at the leading edge of some of those issues.

They also are technologically advanced, and they have a lot of Web access capability in this sector, so they are making use of the technology to deliver services to consumers and to the public, and those are some of the places where, again, the malicious actors have an opportunity to interact with the technology and maybe take advantage of it.

So those are some of the unique challenges, I think. Working with this sector to try to figure out how to do risk assessments and working with them to develop good mitigation strategies is one of the things we are doing at DHS to try to buy down that risk.

Mr. BACA. Let me follow up with an additional question between the Federal Government and the private sector. How does the Federal Government compare to the private sector with regard to receiving, storing, and maintaining encrypted information? And if the private sector has to send or report encrypted data to the Federal Government, can the Federal Government ensure that it remains so protected?

Mr. SCHAFFER. Yes, sir. I believe that the Federal Government has the capability to protect data that is submitted by the private sector. Again, the devil is in the details, and the need to correctly implement solutions and make sure they are maintained in the appropriate way is critically important for any agency that is intaking data.

At DHS, we have some programs that are specifically designed to allow private-sector entities, particularly critical infrastructure players, to submit data with special protections so that they are comfortable with telling us about their security situation without the worry that the information is going to be inappropriately released or made available in ways that could hurt their security over the long run, and we take measures to ensure that we are indeed protecting and maintaining that data in an appropriate way.

The same issue with respect to personally identifiable information that we may come into possession of during our cybersecurity work with other departments and agencies. We have procedures and processes designed to ensure that the data is maintained appropriately and not exposed to unnecessary risk.

Mr. BACA. I realize that my time has expired, but what I heard you make a statement is that we need government involvement, be-

cause everybody says, all right, let's let the private sector separate itself from government and we don't want any more government involvement, but here I am saying that we do need that for that protection versus not to it. One side is saying, all right, let's not allow government to be involved in all regulations; but yet we are saying that we do need it for that protection to allow that safeguard, because the private sector won't be able to provide that kind of protection unless we both have a joint partnership in ensuring we have that kind of security; is that correct?

Mr. SCHAFFER. I certainly think government—

Mr. BACA. We do need government.

Chairwoman CAPITO. The gentleman's time has expired.

Mr. Canseco, for 5 minutes for questions.

Mr. CANSECO. Thank you, Madam Chairwoman.

San Antonio, Texas, is the home of USAA, the largest financial services company in the country. Many of my constituents either work there or do business with USAA, and members of our military and their families have become huge targets for cybercriminals. At USAA, most business is transacted online and with our active and retired military.

Mr. Smith, are there any efforts being made to specifically protect members of our military and their families from having their personal information financial accounts hacked?

Mr. SMITH. Congressman, none that we are not trying to do for the average citizen as well, and a lot of that is again—is just through a public awareness campaign and the things that we try to do, quite frankly, in our electronic crimes task forces. So I wouldn't be able to say that there is specifically for the military personnel.

Mr. CANSECO. Many of them are deployed, either in Iraq, Afghanistan, or in far reaches of the world, and they have their laptops with them, or they have access to computers, and they keep current with what is happening with their financial accounts and when they get deposits and what they have to pay, and they are extremely vulnerable.

Do you think that it is important to make sure that something is done to protect at least our military in a specific way?

Mr. SMITH. Yes, sir, I think it would be good. And, again, just a lot of personal requirement, I guess, on some levels to try to make sure that they are aware of these sorts of things, and that they are, in fact, vulnerable, and that they double-check themselves, as crime prevention goes in terms of passwords, the security of their accounts, and that sort of thing. I think there is something on an individual basis that can be done as well. But I would agree with you.

Mr. CANSECO. Do you feel, Mr. Snow, that the financial services sector is appropriately vetting the background of personnel?

Mr. SNOW. Yes, sir. It is one of the issues that I will bring up. And let me just make a comment about USAA. I know, like many financial institutions, they are very proactive, and they are trying to do everything they can because of their constituency, number one, but because their membership includes others besides those in the military.

We took an individual who came from the Joint Task Force Global Network Operations who went down there to work in that facility and brought him on board for the clearances through the FBI so that we could share that information in realtime. I will go down there for the Cybersecurity Awareness Week in the opening comments just to thank them for what they do for their membership, but also to thank them for being as proactive as they can out there.

But on that line, and we will talk about the vetting first, statutorily there are only certain people who have access to law enforcement records for checking backgrounds. Some of the places like the SWIFT organization that controls the instant messaging going from financial institutions to others don't have that access statutorily. So that is something we need to take a look at.

Also, which I think is interesting to me, after 9/11 we came out with a bill which said we would have off-duty carry for former first responders, law enforcement officers, State, local, and Federal officers, because it would add to our complement throughout the United States a certain response capability. Pilots took weapons after proper training up into aircraft.

What I don't see, and it is interesting to me after having left the military about 25 years ago—when I was in there, I only saw one or two people who had clearances, TS clearances, maybe somebody who was in charge of a certain program, or maybe someone who was a designated intelligence officer. When I went over as the on-scene commander in Afghanistan, I couldn't find somebody that didn't have a TS clearance. So every single fusion center I went into, every single place that I walked into, they carried full credentials.

But now as I reach out, and we are talking about information-sharing, and I try to reach out to people like USAA, we have one member there. What about these other organizations that don't have a government contract, that don't have a military contract, or don't fall into one of the historic arenas where they should have those contracts?

So I have been having discussions on thoughts of, should we carry those clearances on? Maybe somebody leaves the military, and they are going off into a normal business, but 2 or 3 years from now they walk into an area when we see, as Mr. Schaffer says and Mr. Smith says, every agency, every organization, every department, every size business, small, medium and large, and school district, so we could share that information more readily.

Mr. CANSECO. Mr. Schaffer, in your opinion, what cybersecurity roles are exclusively government functions, and which ones are the responsibility of the private sector? And if I am out of time, if you could be brief, please?

Mr. SCHAFFER. Yes, sir. As mentioned in my opening, I think that this is a shared responsibility. In most of these areas, we have to work together. Industry owns the vast majority of the infrastructure. Government has access to certain information, as Mr. Snow just mentioned, some of the classified information that can help make things better. We have to work together as a team. I think that there are multiple efforts under way to make that happen. There are some things that government will do at the classified level, but there is much that we can do as partners.

Mr. CANSECO. My time is up, but I want to thank you three gentlemen for your information very much.

Chairwoman CAPITO. Thank you.

Mr. Carney from Delaware for 5 minutes for questions.

Mr. CARNEY. Thank you, Madam Chairwoman.

I want to thank you and the ranking member for holding this hearing today, and the panelists for coming, and for the great work you do for our country. I am most interested in the threats to our banks and financial services institutions, so I would like to just ask a few questions, really following up on some of the answers that you have already given and your written testimony.

Could you characterize for me—you have talked about individuals, hacktivists, I think you said, nation state perpetrators and organized crime. Who is most involved in the attacks on our financial services, our banking and cyber infrastructure, and how are we doing stopping them and arresting them and bringing them to justice? Maybe we can start with the FBI or whoever feels most comfortable with that.

Mr. SNOW. Yes, sir. I would say right now that the largest threat to the financial services institutes and institutions is from the criminal organized crime group and realm, at least where we have the most information pointing to a specific adversary.

Mr. CARNEY. Are those domestic or offshore organizations?

Mr. SNOW. Many offshore, sir, that we see.

Mr. CARNEY. Most offshore, or how would you break that down as a percentage?

Mr. SNOW. I would say it is probably a 90–10 split, maybe an 80–20 split.

Mr. CARNEY. But overwhelmingly mostly offshore then?

Mr. SNOW. Yes, sir. And it is important to make a distinction, and the distinction would be those that are doing organized criminal groups for profit, and then the hacktivists. So we see a lot of hacktivists who are still worldwide. We have been identifying many here within the United States, but they are not the real threat to the financial institutions and organizations. They are a harassing threat. They cost a lot of money, they do a lot of damage to the systems, but they are not the ones that I guess are damaging the economic stability.

Mr. CARNEY. So how are we doing stopping them and arresting them, whoever is the best one to answer that question, and what, if anything, do we need to bolster our efforts there?

Mr. SNOW. I will make the first comment, sir, and then turn it over to Mr. Smith.

As he stated previously, I think we are doing a good job, especially in the international relations with other countries, working the imbeds, the electronic crime task forces, all the efforts that the United States has as we move from the domestic side out internationally. I think we are doing a good job and a much better job than we have in the past 2 years.

The thing that concerns me is that it is still a reactive mode, so I am trying to find a forensic evaluation of a financial institution. There have been many cases where we have actually gone out to doors and knocked on them and said, here is what we saw in our investigation, and you are already a target through reconnaissance.

Here is what you need to fix yourselves. But I think we need as a government a much more robust effort in that fashion.

Mr. CARNEY. So do you actually arrest these people, find them, or do you just stop them?

Mr. SNOW. We try to arrest them for the deterrence effect. The problem is some countries—and it is a force multiplication—some countries want to prosecute their own individuals, their citizens who reside there. Depending on what treaty or MLAT agreement we have, many may be subject to extradition or not, and others may want to address the issue of their citizens within their domain themselves.

Mr. SMITH. I would agree with Mr. Snow. It just really depends on the country and the level of cooperation. We have had cases in the Secret Service that were very significant, that were large enough that we actually, through some of our undercover operations, were able to lure that individual out of their home country and bring them to the United States in order to be arrested. So it just depends. Each one is sort of an individual case and an individual plan, if you will, to go after them.

Mr. CARNEY. So there is not a pattern there. Are there countries that you would want to point out publicly that are problematic, or is that something you would rather not say publicly?

Mr. SMITH. I wouldn't want to do it individually, but I would say, as we mentioned earlier, a lot of our liaison efforts are in that Eastern European area and also the Baltic region, and that is specifically why we opened our office in Tallinn, Estonia.

Mr. CARNEY. Is there anything that you would like to add?

Mr. SCHAFFER. Congressman, one of the things that I would say is that from a National Protection and Programs Directorate part of DHS, recognizing Secret Service is another part, our focus is on network defense. The attribution pieces we leave to the law enforcement folks for the most part. But what we do try to do is make sure that we are taking the knowledge from one incident within the financial services sector and making it available to the rest of the sector. And in some cases, we have even had the opportunity to bring in an entity that was experiencing an issue that we had seen some months before at another entity and correct those two entities in a way that wouldn't have been possible but for government being able to know about both of the incidents and being able to connect the dots.

Mr. CARNEY. I see my time is up. I want to thank you again, and please feel free to contact us if there is something we can do to help in those efforts. Thanks for those efforts.

Chairwoman CAPITO. Thank you.

Mr. Luetkemeyer for 5 minutes for questions.

Mr. LUETKEMEYER. Thank you, Madam Chairwoman.

Thank you, gentlemen, for being here today.

A lot of questions I was going to ask you have already been asked this morning, so I will try and be brief here.

I am just kind of curious. With regard to financial institutions, are most of the thefts done with inside help, or are they mostly done from the outside?

Mr. SMITH. It is really a combination. I would say most are from the outside. But, again, the insider threat study that was con-

ducted several years ago, which we would be happy to share with you, showed that there is a certain amount of that. And certainly, an insider has access to a lot more information than the outsider. But I think probably in sheer numbers, there are more outside.

Mr. LUETKEMEYER. What do you see as the most exposed? Are the big banks the ones that are mostly attacked, or medium-sized, small banks, because perhaps they are not as sophisticated with their security network? What do you see?

Mr. SMITH. That is one of the things that the Verizon study points out, that a few years ago it was the larger financial sector banks and corporations, but because now they have had time to react to a lot of these sorts of things, we are seeing that more smaller institutions and smaller businesses have become their target. And so we are seeing more of that in this most recent study.

Mr. LUETKEMEYER. Whenever you see that smaller institutions are being attacked, why are they so connected? It would make sense to me that they could—because they are not as large, and they are probably not as integrated, the need for integration probably isn't as great, couldn't they have a separate system that would be inaccessible so that their basic information could be retained and not accessible versus allowing full access to everything? I am pretty naive when it comes to this sort of stuff, so bear with me here.

Mr. SMITH. No, I agree. And I think that they will now have time to react. I think we are all human. Until you become a victim, you don't pay a lot of attention to it, so I guess it was something that was not quite at the forefront of their thinking. Again, it was the larger institutions that were suffering these losses and these hacks, but now in the last year we have seen these smaller institutions become more vulnerable. So I think there are certainly precautions that they can take and should take and probably will do exactly what you are saying in the coming years.

Mr. LUETKEMEYER. I doubt that you guys want to answer this question, so I will just make a comment. If you want to comment on it, you are welcome to. But from the national security standpoint, whenever somebody is trying to hack in, wouldn't it make sense that when they hack in, it would automatically trigger a virus going back the other way so you destroy the guys on the other end?

Maybe you already do that and you don't want to tell me about it. That is fine. It would make sense to me to make sure you make life as miserable on the other end as they make it for us on our end.

Thank you, gentlemen. I appreciate it.

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

Chairwoman CAPITO. Mr. Green from Texas for 5 minutes.

Mr. GREEN. Thank you, Madam Chairwoman. I especially thank you and the ranking member for allowing me to participate in this hearing. It is exceedingly important that we have this opportunity to explore these issues, and I thank you very much.

To the members of this panel and the next, I thank you for appearing here today.

The intelligence that I have received and perhaps has been shared bears repeating if it has: $388 billion lost last year to cyber crime, $114 billion in the United States alone; 1 million new cyber victims per day, that is very daunting; and 54 percent of these cyber crimes can be easily prevented, according to what has been shared with me.

Notwithstanding these stats, I do believe that we will prevail, and I say this to you because I am confident that when we moved from coins to paper, someone and some people said, my God, that paper will never work, it is too easy to duplicate. Then when we moved from paper to checks, someone said, our checks are too easy to write, it will never work. As we moved into the plastic era, there were always people who thought that plastic would never compete with paper. But the truth is we have been successful, and I think we will be successful with these efforts and these endeavors, notwithstanding statistics that are daunting.

I am confident that privacy is something that you have considered, and it is a real issue, and my hope is that the champions of privacy, those who wake up every morning and they eat and they sleep privacy, my hope is that they have been included within those who are part of this avant-garde effort. My belief is that you have done it, but I will just ask anyone who would like to respond to tell me about the efforts to bring in the organizations that make it their daily responsibility to protect the privacy rights of Americans. Are they involved?

Mr. SCHAFFER. Congressman, indeed we have made an effort to include the privacy community in many of the efforts that we have under way at the Department of Homeland Security. Many of the systems that we deploy, like the intrusion detection systems and intrusion prevention technologies that are being deployed for the government networks, we have done privacy impact assessments that have been made publicly available. We have briefed those in the privacy community. We have brought the privacy community in to look at a lot of what we are doing programmatically.

We also have privacy officials within the Department who are tasked with making sure that, in fact, as we go forward on cybersecurity issues, we are looking at the privacy implications of those issues and making sure that they are addressed as we go forward in many of these areas. So we have spent a lot of energy trying to ensure that privacy is considered at each step of the process.

Mr. GREEN. Thank you.

Let me move quickly to tools. I trust that we are giving you the necessary tools that you need timely. Are there tools that you need, laws that you need from Congress, or is there something that we should be doing or paying special attention to so as to make your efforts successful?

Mr. SMITH. If I could, Congressman, I would respond to that and I would just say that, yes, we are receiving, I think, the support that we need. But one thing I would like to highlight is that the Administration has proposed data breach legislation that goes a long way toward improving some of these things that you are talking about, and certainly would aid law enforcement if this sort of legislative package were passed.

Mr. GREEN. Thank you.

And finally, extradition. I know that one of the big problems that you have is that the person who commits the dastardly deed is in some distant place beyond our borders, and if prosecuted may not be extradited to this country. I know that is a real concern for you. Could you just elaborate on it for just a moment, please, as my time is expiring?

Mr. SMITH. Just to follow up again, it really depends on the individual country, and that is why we try our very best with our liaison efforts, the agents. We have 74 agents overseas assigned to different countries, and they work every day toward trying to improve those kinds of relationships. Again, we could give you a specific briefing outside of this forum if you would like on kind of our successes or negatives there.

Mr. GREEN. Thank you very much. Because my time is about to expire and I am an interloper, let me just thank all of you and thank the Chair again because my time is up. Thank you very much.

Chairwoman CAPITO. Thank you.

Mr. Pearce from New Mexico for 5 minutes.

Mr. PEARCE. Thank you, Madam Chairwoman.

If I could get each one of you to kind of give me an idea, just a percent, what percent of the cases that come across your desk do you actually prosecute, and then what percent do you actually convict? Just a rough guess.

Mr. SCHAFFER. I can go first, because my answer is easiest. We don't have law enforcement authority within my part of DHS, so we are not in that business. I was a Federal prosecutor at one point on these issues back at the Justice Department, but these gentlemen have the ball on this one, sir.

Mr. SMITH. It is sort of a splintered answer, if you will, because we obviously have jurisdiction in a number of areas. I can tell you that we arrested over 1,200 people for cyber-related crimes last year, and that resulted in a loss of about $500 million, and we think we prevented about $7 billion in loss just in Secret Service cases. But I could certainly get you our exact number in terms of both arrest and conviction.

Mr. PEARCE. We are, say, saving $7 billion out of $388 billion. That is modest.

Mr. SMITH. Yes, it is.

Mr. SNOW. Yes, sir. I would echo the same. I can always come back with the actual numbers for you later on. My portfolio runs everything from intrusions down to Internet fraud. Many, many cases are prosecuted at a high level, NSM images, child exploitation, some of the intellectual property rights. And some of the national security stuff, for obvious reasons, does not reach that same threshold of prosecution. And then on the criminal side, I think we have had success, but I would have to get you the actual numbers.

Mr. PEARCE. Mr. Schaffer, what do you all do with them when you get them, when you find them? What do you do with them, since you don't prosecute them?

Mr. SCHAFFER. Yes, sir. We have representatives from both the FBI and the Secret Service on our watch floor, so law enforcement is coordinated with us, and we work with them on the issues that

we discover that are reported in to our processes. It is a coordinated effort

Mr. PEARCE. You refer them over?

Mr. SCHAFFER. Yes, sir.

Mr. PEARCE. So if we have a pretty small, modest prosecution rate and an even smaller conviction rate, what is our awareness rate? What percent are we aware that is going on, and what do we don't even have a clue is coming in the attacks? Is that large, small?

Mr. SCHAFFER. Sir, I think that one I can address, which is we know what we know about, and the reporting—there is no requirement currently for private-sector entities to report when these incidents occur, at least from a DHS perspective. We work in partnership. We get a lot of reporting from the private sector when incidents occur, and we work with our law enforcement partners, and we get awareness through that, and we get awareness—

Mr. PEARCE. Excuse me, my question is that we don't know what is even occurring. You wait for a report to come in after somebody discovers that it has happened, and I am asking, how many attacks are coming in, how many attempts are coming in that we don't even know about? Do we actually have a chance to prosecute a very small percentage of that? If so, then the magnitude of the problem is much bigger. I don't want to get much deeper into it. I think I understand.

Has the Treasury, Mr. Smith, ever lost money? Have they been hacked like an individual? Has anybody been in there borrowing money?

Mr. SMITH. Not to my knowledge, Congressman.

Mr. PEARCE. Okay, just checking.

How many times have you individuals sat down at the table together, the three of you, before this meeting today?

Mr. SNOW. I would put it up at about 150 to 200 times.

Mr. PEARCE. So the agencies are cooperating, and we are not all chasing the same guys?

Mr. SNOW. No, sir. Sometimes we have meetings even when we don't want to have meetings.

Mr. PEARCE. That is nice.

How many attempts have been made on the electrical grid? Do you all track that?

Mr. SCHAFFER. Again, sir, we know that there have been attempts made. We know about instances when various parts of the electric grid have been subject to attack. I can't tell you how many attacks have occurred that we don't know about, but I do know that has been happening.

Mr. PEARCE. Have we seen blackouts because of those attacks?

Mr. SCHAFFER. I can't speak to specific blackouts in the United States that are caused by a cyberattack at this point.

Mr. PEARCE. My belief might be that our greatest threat would be the interruption of electrical services. It would affect everything in the country immediately. Is that the perception you all talk about? Would you all perceive that to be an accurate or inaccurate statement? And then, what are we doing to protect that grid?

Mr. SNOW. Sir, I would say that is an accurate statement. I would say that is a big concern, industrial control systems, data

systems, process control systems. I will put a kudo in to the Department of Homeland Security which has a very robust response capability. They have trained most of our cyberaction team individuals for response on that issue itself. And I can tell you in no uncertain terms that when a blackout happens, my BlackBerry goes off, and one of my first calls is back over to DHS, and whether it is overseas, through one of the legal attaches or one of the domestic offices, those people are woken up to get your contacts and find out exactly what that is.

Mr. PEARCE. I appreciate each one of you, and I appreciate especially that you have been cooperating together and working across those jurisdictional lines. That is a frustrating thing from this side, when agencies don't even talk to each other and you have similar threats or the same threats.

But thank you, Madam Chairwoman, for your indulgence.

Chairwoman CAPITO. Thank you.

I want to thank all of the Members, and I want to thank the members of this panel. The first panel is dismissed.

I do want to make a quick comment. We have talked about what threats there are to individuals. I mentioned in my opening statement that I thought I was one of these folks. I think I certainly have been. But certainly, whether my MasterCard has been compromised pales in comparison of what could happen to our country if a financial cyber crime of a large scale is perpetrated. And I don't think we really think about it in terms like that.

I want to thank you. I know you think about it like that, and I am glad you are thinking about it in those terms, because it could really seize up our country. It could go into things like electrical interruption and everything else. Because I don't think we really, at least speaking for myself, have a total concept of all of the financial business that is conducted over the electronic payment systems and through our computers.

So thank you very much for doing this. I know it is very complicated, and I know you are chasing a lot of 20-year-olds at the same time sometimes in these cyber crimes, and that is difficult. So I appreciate your forthrightness and your testimony. And I would like to call up our second panel of witnesses. So thank you all very much.

At this time, I would like to welcome our second panel of witnesses. I appreciate you gentlemen coming today to educate us on this very important issue.

I will introduce each of you individually for the purpose of giving a 5-minute statement. I think you heard me mention earlier that we have your written statements for the record, and we will try to keep our opening statements to the 5-minute deadline.

Our first witness is Mr. William B. Nelson, who is president and chief executive officer of the Financial Services Information Sharing & Analysis Center. Welcome.

STATEMENT OF WILLIAM B. NELSON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, THE FINANCIAL SERVICES INFORMATION SHARING & ANALYSIS CENTER (FS–ISAC)

Mr. NELSON. Thank you, Madam Chairwoman and Ranking Member Maloney. Thank you for inviting us here today.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 that called for the public and private sector to work together to address cyberthreats to the Nation's critical infrastructures. After 9/11, in response to the Homeland Security Presidential Directive 7 in the Homeland Security Act, FS-ISAC expanded its role to encompass physical threats to our sector also.

FS-ISAC is a 501(c)(6) nonprofit organization that is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial institutions. Since that time, the membership has expanded to over 4,200 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payment processors, and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC works closely with various government agencies. I think you heard in the prior panel who we work with. A complete list of the FS-ISAC sharing services are included in my written testimony. I am going to highlight a couple of those key services.

I think one of the key ones is the delivery of timely, relevant, and actionable cyber and physical email alerts from various sources—actually, hundreds of sources. We have an anonymous and attributable online submission capability to facilitate member sharing of threats and attacks. We operate an email list-serve supporting attributable information exchange by various special interest groups. Surveys allow members to request information regarding security best practices at other organizations. And then, we have a biweekly threat information call. We have emergency threat or incident notifications and conference calls. And we have special projects to address specific risk issues, such as the Account Takeover Task Force, which was mentioned in the earlier panel.

We have implemented a number of programs in partnership with DHS and other government agencies. We have, actually, representation on the National Cybersecurity and Communications Integration Center, the NCCIC, watch floor. These are FS-ISAC representatives cleared at a Top Secret/Sensitive Compartmentalized Information level, or TS/SCI.

It should be noted that the FS-ISAC has worked closely with DHS, the U.S. Treasury, the FBI, the Secret Service, and other government partners to obtain over 250 Secret-level clearances and a number of TS/SCI clearances for a number of key personnel.

An example of a successful instance of government and financial services sector information-sharing occurred on October 24, 2009, when the FBI, the FS-ISAC, and an organization called NACHA, the rulemaking body for the ACH, released a joint bulletin concerning account takeover attacks targeting businesses and corporate customers. Some of those—actually, details of those recommendations are not included in my testimony, but they included: initiation of ACH and wire transfers under dual control; reconciling all banking transactions on a daily basis; implementing customer awareness programs; actually implementing fraud detection and mitigation best practices, including anomaly detection; and out-of-band authentication of transactions.

It is my understanding that the OCC is not here today, but I would like to talk about the recent FFIEC supplemental guidance on Internet banking authentication. It incorporates many of the defense-in-depth recommendations that were included in our bulletin with the FBI and a number of important new regulatory provisions. It calls for, actually, annual risk assessments by financial institutions. It now distinguishes between retail and commercial accounts, actually raising the bar of minimum controls for all accounts and recognizing that commercial accounts pose a higher level of risk. It also insists that financial institutions have layered security for consumer accounts.

I think the thing to point out is, this goes into effect in January 2012. And they use the word "guidance," but it is actually a requirement. All financial institutions were required to adhere to this.

I also in my written testimony talk about the Account Takeover Task Force. We had over 120 individuals from 35 financial firms, 10 industry associations and processors, plus representatives from 7 government agencies participate in that task force. And they developed a number of important deliverables, including—major deliverables, including how to respond, prevent, and detect different types of cyber attacks.

Lastly, I just wanted to mention we have conducted a cyber attack payment exercise in 2010. We are planning another one this year in November.

And, with that, I just want to wrap up and conclude that I think before 2009, the corporate and consumer public knew very little about the risk of cyber crime. I think that joint bulletin was the beginning of a massive educational effort that has been somewhat effective in raising awareness of financial institutions and their customers of cyber crime attacks. Since then, we have worked with the FBI, the U.S. Secret Service, and DHS to issue new bulletins. This cyber attack exercise, the FFIEC supplemental guidance, and the deliverables of the Account Takeover Task Force have all played important roles in increasing that awareness. I think today more financial institutions and their customers are now aware of how to detect, prevent, and respond to malicious and criminal activities resulting from online attacks.

Thank you again for this opportunity to present this testimony, and I look forward to your questions. Thank you.

[The prepared statement of Mr. Nelson can be found on page 64 0f the appendix.]

Chairwoman CAPITO. Thank you.

Our second witness is Mr. Bryan Sartin, director, investigative response, for Verizon.

Welcome.

STATEMENT OF A. BRYAN SARTIN, DIRECTOR, INVESTIGATIVE RESPONSE, VERIZON

Mr. SARTIN. Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee, thank you for the opportunity to testify here. My name is Bryan Sartin, and I am director of investigative response at Verizon.

Verizon is a global provider of communication services. Our data network spans 6 continents and 150 countries. As detailed in my written statement, we engage in a wide range of activities to enhance cybersecurity both for ourselves and for our customers.

Investigative Response is a specialized group of IT investigators who handle more than 200 cases each year, including many highly visible data breaches. Our findings are documented in a Verizon "Data Breach Investigations Report." It encompasses more than 1,700 data breaches over 7 years of research. It is a study about security failures and the lessons we can learn from them.

This report provides valuable guidance for corporate and government entities on effective ways to secure their networks, including financial services firms. The report utilizes an information-sharing framework that we developed called Verizon Enterprise Risk Incident Sharing, or the VERIS framework, which we have published as an open-source initiative.

There are five points that I would like to share with the subcommittee today.

Point one: Although the consequences of cyber attacks may vary depending on the target, there is little variance in cyber risks and threats by sector. Hospitality, retail, and financial services are the top three sectors in terms of data-breach victims. Cyber criminals are after data they can easily convert into cash. More than 90 percent of electronic crimes are, in fact, financially motivated. Retailers and financial services entities have the largest quantities of targeted data types, namely credit card, debit card, and PIN information that we see targeted in nearly 80 percent of our cases.

While those two sectors will continue to be key targets of electronic crimes, they do not face a unique cybersecurity threat. Cyber threats are neither sector-specific nor unique; they are mostly opportunistic and blind to industry.

Point two: Electronic crimes generally do not involve complexity or innovation. Nine of the top 10 hacking methods are, in fact, very simple. For example, criminal exploitation of default or easily guessable credentials accounted for nearly two-thirds of our cases. Many devices come with default user names, such as "Admin" or "Password1," and, if left unchanged, these default credentials offer cyber thieves often easy entry points into potential victim systems.

Point three: The most fundamental security controls make the most effective countermeasures. Over 70 percent of criminals' points of intrusion are through victims' own remote-access facilities. It is not that the technologies are flawed. Instead, it is the manner in which they are deployed and the way they are configured. Most criminal entry can be prevented if a second factor for authentication is required. For example, if a system requires a username and password and the additional requirements of a hardware or software token, it would prevent most remote-access intrusions that we see.

Now, making it difficult for criminals to exfiltrate stolen information is another simple but highly effective way to prevent data breaches.

Point four: There is often a significant time lag between when a breach occurs, when data theft actually occurs, and when the victim finds out. The timeframe from initial point of entry to the first

instance of data theft is more often measured in days, weeks, or months as opposed to minutes or hours. On average, it takes victims more than 6 months to discover that they have been hacked into. Even after 6 months, almost 9 out of 10 victims did not make that discovery on their own; they found out from third parties. Significant improvement in data-breach detection is badly needed.

Point Five: Closer cooperation between victims and law enforcement could reduce the overall numbers of electronic crimes. Greater information-sharing has improved our ability to identify criminals conclusively, and that is critical to successful prosecution and, in turn, has had a huge impact in reducing cyber crimes.

The greatest obstacle to cooperative information-sharing is the reluctance of victims to engage law enforcement for fear of fines, penalties, and litigation. And reasonable protections from litigation and regulatory fines would encourage victims' cooperation with law enforcement that would improve the odds of successful prosecution and reduce the overall numbers of overall electronic crimes.

In conclusion, cyber attacks represent very real threats to our economic prosperity and our Nation's security. While many public- and private-sector remediation activities have been highly effective, our investigations indicate that greater vigilance is required.

The data-breach report lays out several recommendations which, if implemented, would improve the cybersecurity posture of financial services firms specifically and of all entities more generally. Overall, every entity must identify a set of essential controls and ensure their implementation consistently and without exception. More advanced controls can be implemented as necessary. Achieve "essential" first and worry about "excellent" later.

Madam Chairwoman, thank you again for this opportunity. I look forward to answering any questions you may have.

[The prepared statement of Mr. Sartin can be found on page 101 of the appendix.]

Chairwoman CAPITO. Thank you.

Our third witness is Mr. Brian Tillett, chief security strategist, public sector group, Symantec.

Welcome.

STATEMENT OF BRIAN TILLETT, CHIEF SECURITY STRATEGIST, PUBLIC SECTOR GROUP, SYMANTEC

Mr. TILLETT. Thank you.

Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee, thank you for the opportunity to appear before you today as the subcommittee considers cybersecurity and threats to the financial sector.

My name, again, is Brian Tillett, and I am the chief security strategist for the Public Sector Group at Symantec. Symantec is the world's information security leader, with a footprint of more than 200,000 sensors in more than 200 countries and territories which track malicious activity globally 24 hours a day, 365 days a year. We refer to this as the Symantec Global Intelligence Network.

At Symantec, we are committed to assuring the security, availability, and integrity of our consumer, enterprise, and government

customers' sensitive information. Concurrently, protection of critical infrastructure in all sectors is a top priority for us.

In my testimony today, I will provide the committee with an abridged analysis of the threat landscape, an assessment of threats in the financial sector, and risk-mitigation measures for addressing those threats.

The threats landscape is constantly evolving. In the most recent "Symantec Internet Security Threat Report," which we publish annually, we observed significant shifts in 2010. The volume and sophistication of threat activity increased more than 19 percent over 2009, with Symantec identifying more than 286 million variations of malicious software, or malware. To put it in another perspective, that is a staggering 9 per second. These included threats to social networking sites and their users, mobile devices, and targeted phishing attacks. Symantec intelligence quarterly reports indicate that these trends are continuing at an accelerated pace through 2011.

We have observed an ominous change that has swept across the Internet. The threat landscape, once dominated by worms and viruses developed by irresponsible hackers, is now being ruled by a new breed of cyber criminals. Just last week, we released the "2011 Symantec Norton Cyber Crime Report," where we calculated the cost of global cyber crime at $114 billion annually. We also calculated that lost time due to recovery and impact on personal lives was an additional $274 billion worldwide. With an annual combined cost of $388 billion, cyber crime costs are significantly more than the global black market of marijuana, cocaine, and heroin combined.

We also have been monitoring an array of threats specific to the financial sector for many years, including ATM heists, banking trojans, and botnets. These threats will only continue to mature and increase as society becomes more dependent on technology for financial and banking needs.

Let's address a snapshot of the recent trends. We have talked a considerable amount about botnets already, so I am going to skip through some of the background on this, but I wanted to add some more context: that botnet owners are often known to rent the use of their botnet to other users. And they will do this in an effort so they can perpetrate malicious activity, also reinforcing the fact that you do not have to be an uber-hacker in order to perpetrate malicious activity. We saw evidence of this in the denial-of-service attacks on the payment card industry after WikiLeaks events last year.

One such botnet targeting the financial services industry is called Qakbot. It is a sophisticated malware that has been spreading through shared networks, thumb drives and infected Web pages since 2009. Among other things, where it is trying to steal financial information, one of the things it likes to do is it will hide the log-out button when you are actually signed into your favorite financial institution, perhaps Bank of America, and it will actually intercept that log-out transaction, and phone home to its command-and-control infrastructure server, and say you can now log in using the credentials that someone else is using. That is another characteristic of the Qakbot botnet.

Trojan horses are another type of malware that is designed to look like a valid or beneficial application, or perhaps an app that you would put on your mobile device, and sometimes even act the way that they are expected. At the same time, they introduce a hidden malware into the enterprise designed to seek sensitive financial and other high-value info and exfiltrate that from the enterprise in a covert fashion.

As more users download and install third-party applications for mobile devices, the opportunity for installing malicious applications is also increasing. There will likely be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking.

As a sign that the mobile space is starting to garner more attention from cybercriminals, there was a 42 percent increase in the number of reported new mobile operating system threats and vulnerabilities from 2009 to 2010. We also see that increasing, as our study in 2011 shows.

There is no one-step program for mitigating risks to the financial sector, and while it is leaps and bounds ahead when it comes to security, there are still steps that need to be taken to lessen the impact and prevent future attacks. In our written testimony, we have provided recommendations on how to better protect critical systems from cyberattack. Embracing new technologies and other technological improvements are necessary, but they must be paired with increased education and awareness.

In addition, there has been progress over the years to advance information-sharing among critical infrastructure sector partners and the government. Private-sector alliances such as the National Cyber Forensics and Training Alliance and the Financial Services Information Sharing & Analysis Center have done a commendable job of creating mechanisms to share intelligence among industry and between industry and government.

Successful mitigation of the threats to the financial sector depends on this continued communication; however, information must be shared in a timely and actionable manner. There are still significant impediments to government sharing information with industry, including classification designation, legal restrictions, and competitive advantage concerns.

I applaud the committee's commitment to this critical topic and its leadership on information security issues. As the threats we face today escalate, we must continue our informationcentric cybersecurity strategy, improve information-sharing mechanisms, and increase awareness in education. Symantec looks forward to continuing to work with Congress and our partners to address these important issues.

Thank you again.

[The prepared statement of Mr. Tillett can be found on page 149 of the appendix.]

Chairwoman CAPITO. Thank you, Mr. Tillett.

Our fourth witness is Mr. Greg Garcia, partnership executive for cybersecurity and identity management, Bank of America.

Welcome, Mr. Garcia.

STATEMENT OF GREG GARCIA, PARTNERSHIP EXECUTIVE FOR CYBERSECURITY AND IDENTITY MANAGEMENT, BANK OF AMERICA

Mr. GARCIA. Thank you, Chairwoman Capito, Ranking Member Maloney, and members of the subcommittee. I am Greg Garcia, partnership executive for cybersecurity and identity management at Bank of America. I also serve as co-chair of the cybersecurity committee of the Financial Services Sector Coordinating Council.

Thanks again for inviting me to discuss cybersecurity with the committee. I will provide a quick overview of the cybersecurity threat environment; how Bank of America manages security to protect our company, our customers and our shareholders; and how we partner with industry and government to mitigate the cyber risk.

As you know, the global financial system operates on a vast network of information and communications technology. Trillions of dollars in transactions flow across the network globally on a daily basis. It is our responsibility to ensure the swift delivery of those services wherever we do business, to secure the data and networks that enable them, and to prevent unauthorized access that could lead to fraud, identity theft, data loss, or system downtime.

At Bank of America, we are laser-focused on cybersecurity. In discussing how we manage this challenge, it is useful to break it down into two interrelated components: one, our customer facing policies and activities; and two, our enterprise-level security. Of primary importance to us is securing our customer financial information. We take this very seriously, and we invest heavily to protect our customers, and we deliver a range of services to secure their transactions and to keep our consumers whole, such as fraud monitoring and zero dollar liability guarantee.

In addition, we offer more than 50 kinds of alerts to our customers to choose from, including alerts that will notify you if there is irregular activity on your account. In fact, Javelin Research designated Bank of America number one, best in class, in security and privacy for online for our consumers for the fifth year in a row, and we are quite proud of that. We have done a lot to achieve that.

We also continue to educate our customers with many tips about what they can do online to protect themselves online and in the mobile environment, and we offer additional tools such as antivirus protection for them to use.

We continually warn our customers about phishing—you have heard a lot about that already—which remains one of the most widely used and effective attack methods by cybercriminals. Those are simply targeted emails that look legitimate, but they trick receivers into clicking on malicious links or entering personal information, and these are difficult to spot and to prevent. But again, with our awareness regime program, customers who are victims of fraud are not liable for fraudulent transactions, and they are protected with the zero liability guarantee.

Our customer-facing security strength relies on many of the standards of practice that protect and enable our broader enterprise. Our security strategy is designed to protect critical nonpublic data, intellectual property, and operational availability and continuity. It is in all of these areas that we work very closely with

our regulators to ensure that we apply, maintain, and constantly measure all the necessary security controls across the enterprise.

Much of our work in security is aimed at addressing the increasingly sophisticated threats from well-organized and funded groups that you have heard about earlier today, and to stay ahead, we are continually investing in new tools and new capabilities and the highest standards of practice commensurate with the financial sector status as critical national infrastructure.

We are on alert 24 hours a day, 7 days a week. Fundamentally, our cybersecurity program is based on a combination of people, process, and technology. Let me just summarize what that means in high points.

Across the company, all employees receive annual training on the importance of information protection, the policies and methods that the bank uses, and the responsibilities of every employee. We have an information security team of experts who have past careers in law enforcement, the military, security, and high technology innovation. We operate under detailed, rigorous information security policies with a program designed to protect the security and confidentiality of customer and client information, and we are concerned about the life cycle of that information from acquisition to use and from storage to disposal. And as we are a global company, and the threat is global in nature, we are building this protective capability wherever we do business.

A few quick words about partnerships: A critical element of a mature cybersecurity program is our investment in partnerships. At Bank of America, we are sharing information and best practices across the financial and other critical sectors and with the government to gain the broadest view of the threat landscape. We do this to get collectively smarter and better at protecting assets and critical information.

For example, you have heard about them in previous statements. We are partnering with the Financial Services Sector Coordinating Council, or FSSCC, the FS-ISAC, the Treasury Department's Office of Financial Services Critical Infrastructure, Homeland Security, and various law enforcement partners globally. These are essential elements in our ability to protect our company, our customers, and our shareholders. They are an opportunity for us to improve our own internal security capabilities and to extend our expertise to other partners. As Under Secretary Schaffer said, no one entity has all the information. It takes teamwork to bring all the pieces together.

So I am proud to say that Bank of America focuses a tremendous amount of resources and energy to stay ahead of the cybersecurity challenge, and we are continually making the necessary investments in developing new tools, processes, and expertise to meet the challenge.

I will conclude my remarks, Madam Chairwoman, and I would be happy to answer questions.

[The prepared statement of Mr. Garcia can be found on page 54 of the appendix.]

Chairwoman CAPITO. Thank you.

Our next witness is Dr. Greg Shannon, chief scientist, Carnegie Mellon University's Software Engineering Institute CERT Program.

Welcome.

STATEMENT OF GREGORY E. SHANNON, CHIEF SCIENTIST, CARNEGIE MELLON UNIVERSITY'S SOFTWARE ENGINEERING INSTITUTE CERT PROGRAM

Mr. SHANNON. Thank you, Chairwoman Capito, Ranking Member Maloney, and subcommittee members. I am honored to testify on the evolving cybersecurity threat to the financial community.

CERT was created in 1988 in response to the Morris worm incident, and we have grown into a national asset in cybersecurity with 200 staff, most of whom are cleared, supporting the operational and R&D needs of our mostly government customers.

When DHS created US-CERT, it called upon CERT to contribute cybersecurity expertise. Through US-CERT, we work jointly with DHS mitigating cybersecurity threats. Please note that US-CERT and DHS work together closely, but are distinct partners who have different roles in providing cybersecurity to the Nation.

To achieve CERT's cybersecurity mission, we engage both public and private communities to create mutable technologies, apply them to real problems, and amplify their impact by promoting broad national and international adoption.

In response to your opening comments, we work with government customers to find practicable solutions to problems like protecting sensitive information that has been aggregated, such as that considered by the Dodd-Frank legislation. Similarly, over 200 computer security incident response teams around the world at the national and sector level can trace a pedigree back to the DOD-sponsored CERT program at Carnegie Mellon.

Our solutions stem from long-standing collaboration and trusted relationships. Those associations give us the opportunity to access real data for our research and development, which in turn enable usproduce operationally viable cybersecurity solutions for the country.

We know that understanding a cybersecurity threat is more than just anecdotes and scare tactics. We know the threat is real and it is evolving, because for—as one example, CERT catalogs over 250,000 instances of malware artifacts each month. As you might imagine, at this volume it is difficult to determine in real time the operational relevance of each artifact. Unsurprisingly the limits in our technical abilities coincide with the steady corporatization of cybersecurity attacks, as we have heard today.

In reference to Mr. Smith's earlier testimony, I just want to acknowledge our work at insider threat and refer you to our testimony there.

The financial sector needs networks that are secure and resilient in order to mitigate escalating cyberthreats. As software vulnerabilities continue to grow at an alarming rate, it is imperative that we build security into the software development process to root out the problem at the beginning instead of responding to the consequences.

CERT, taking a comprehensive approach to limiting vulnerabilities and other software defects, created new international coding standards, developed in coordination with security researchers and software developers, which, when applied, result in more secure systems. There is no magic bullet. Systems will fail, and we need to ensure that business goals are met and critical business functions are sustained despite the presence of cyberattacks. Systems must be resilient. Improving survivability in the presence of cyberattacks also improves the ability of businesses to survive accidents and systems failures that are not malicious.

Through our collaboration with the financial community, CERT has a definition for operational resilience management known as CERT-RMM, and we are quite proud to have worked with the broader community in creating that.

When a cyberattack does occur, we need the forensic ability to locate the source of the attack and limit the damage, sometimes in minutes or seconds, as discussed earlier. As you are aware, computer forensics labs are constrained by the lack of resources and unable to handle the overwhelming increases in volumes of data that need to be examined for evidence; for example, hundreds of terabytes of data captured at data centers by law enforcement.

Partnering with Federal agencies and law enforcement, CERT is creating solutions to enable organizations to accelerate the tempo of investigations, as well as boost computational analysis of the data. CERT is currently working on a new incident analysis framework which speeds up the velocity of investigations and allows for faster and more adaptive defense and mitigation opportunities otherwise not available in near real time.

These examples of CERT's work highlight the need for leadership and support from the government in policy discussions about research and about how research can support sound policy decisions in cybersecurity. Research is only as good as the data it is created from, and currently, researchers have limited access to data. To better combat the cyberthreat, we must maintain better situational awareness, otherwise policymakers and experts are left to speculate about what is the right data to share. Achieving this enhanced situational awareness will require continued research on network data and the cooperation of the financial community.

The credit card fraud detection capabilities that were referred to in opening remarks is a good example of public-private research and development that started 20 years ago in the financial community, and I think can serve as an example of addressing issues in cybersecurity.

I realize information-sharing on this scale tends to exacerbate an already contentious relationship between security and privacy. This is an unhealthy condition, and our adversaries are exploiting it. In an ever more interconnected world, anonymity is being redefined, and, without security, there is no privacy.

We at CERT look forward to working with the Federal community and staff and other stakeholders to improve the security and survivability of our national assets.

Thank you.

[The prepared statement of Dr. Shannon can be found on page 118 of the appendix.]

Chairwoman CAPITO. Thank you.

Our final witness is Mr. Marc Rotenberg, executive director, Electronic Payment Information Center.

Welcome.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

Mr. ROTENBERG. Madam Chairwoman, Ranking Member Maloney, thank you for the opportunity to be here today.

EPIC was established to focus on emerging privacy and civil liberties issues. In fact, the first issue that we took on was the availability of the strong technique for data security encryption, because we understood that this was critical for the development of the Internet and its use as a platform for commerce.

I also wanted to thank the subcommittee for your interest in this issue and acknowledge the important work of the witnesses on the first panel on the law enforcement side protecting the interests of American consumers.

I would say from the consumer perspective, this is one of the most critical issues people face today. As the earlier witnesses have stated, the loss in dollar amounts are very high. According to the Privacy Rights Clearinghouse, over the last several years, more than 500 million records containing sensitive personal information have been lost in data breaches.

We know in addition to the recent hacks of financial institutions, there are also non-financial institutions that contain a great deal of sensitive financial information. For example, the Sony PlayStation Network, which was compromised, contained credit card record information, and contained unencrypted password files that were accessed. These are very sensitive and significant issues.

And then, of course, most recently involving the so-called Comodo hacker, the digital certificates which provide the basis for a lot of the trust and confidence in the online environment were compromised as well. These are the techniques that make it possible for a person to go to a Web site that says Google or Yahoo or Skype and be assured that it is, in fact, the Web site of the company that is being represented.

So the urgency here is clearly quite significant, and if this is not enough to worry about, I would suggest to the subcommittee as well that you may also need to look at the cybersecurity implications of moving more commercial data, more of the government's data, and more consumer data into the cloud computing environment. One of the practical consequences of the migration of this sensitive personal information is that it will be more difficult for consumers and government agencies and businesses to be aware when this kind of activity occurs because it will no longer be the data that is in their possession.

Now, in my prepared statement I offered a few suggestions of legislative principles. I understand the hearing is not primarily focused on legislation, but I would like you to consider that when consumers turn over their personal information to financial institutions, there is actually very little that they can do at that point to safeguard their information, and that is the reason that we have recommended to other committees and would recommend to this

committee as well that you consider strong legislative safeguards to protect the information of consumers that is now in the possession of financial institutions.

So, for example, we favor an opt-in standard so that people are aware when their personal information is disclosed to others. We favor strong breach notification so that people know when these kinds of incidents have occurred. We think it is important also that States remain free to develop their own legislation to protect consumers.

There is oftentimes an effort in this area to establish a so-called national standard, but one of the practical problems because the threats are so quickly evolving is that a single national standard, unless it operates as a baseline, may actually not be adequate to deal with some of the new threats.

California, for example, had to recently amend its breach notification law so that people would be more fully informed about some of the risks if their personal information was disclosed, and what additional steps they might take to protect their information. I think it is also interesting that in the California law, there was an obligation on institutions in the financial services sector that suffer a breach to notify the State attorney general so that the State attorney general would have a clearer picture across the State of a pattern of breaches that had occurred, and what additional efforts the States may need to take.

I think that is actually a very helpful approach going forward, as you think about cybersecurity, how do you get a good assessment of where the risks are, what the harms are, and what additional steps might be taken.

So, again, I am grateful for the opportunity to testify today. I would say for American consumers, the protection of their financial information has to be one of the top concerns.

[The prepared statement of Mr. Rotenberg can be found on page 88 of the appendix.]

Chairwoman CAPITO. I couldn't agree more, and that is a good place to stop.

I want to thank all of you for your testimony. I am going to begin the questions.

Mr. Garcia, first of all, I would like to thank you and Bank of America for coming forward in this particular panel, realizing that acknowledging security breaches are difficult for competing entities. And Mr. Rotenberg talked about retailers, same issue. If you are perceived to be a company that has a weak cybersecurity wall or breaches of personal information, you are obviously going to lose customers or lose people who come into your store or wherever. You have received an award, your bank has, and you are obviously on top of this.

When a breach occurs, no matter what the magnitude, what are you actually required to do in terms of notifying your customer, or notifying the FBI, or notifying Mr. Nelson's organization? I am assuming you are one of his members. What are you required at this point to do?

Mr. GARCIA. We have a number of requirements on a per- State basis, of course. Where we operate, there are State breach notification laws. Also, under the FFIEC, as was mentioned by Bill Nelson,

there are requirements whenever we have an event, we notify our regulators.

Chairwoman CAPITO. Your regulators.

Mr. GARCIA. Correct. So we have a very well-defined, tightly scripted set of requirements and routines for when we have a breach and how we work with law enforcement, what we do with that information internally and—

Chairwoman CAPITO. What about with your customer? Does the customer have to opt into being notified, or you are required to notify them no matter what?

Mr. GARCIA. Not no matter what. We work with law enforcement. When an investigation is under way, we want to be sure that we don't flood customers with false information. So we want to be sure that they have confidence that their information is being well handled. But the important thing is making sure we provide the customer accurate and actionable information, if something actually has occurred.

Chairwoman CAPITO. I am not going to ask about mobile devices, but I am very curious about them. I think that is probably a signal of my age, wondering, gosh, we are going to be able to actually carry that around and do all those kinds of things? But I think you all have voiced a concern about where that is going to lead, and I think from the last panel, he mentioned that we need to be on the front end of that in terms of trying to prevent fraud, rather than reacting to it once it occurs, because we know it is going to occur. Somebody said 52 percent more threats to the mobile—I think that might have been you, Mr. Tillett.

In the Dodd-Frank Act—and I don't know if you are familiar with this—an Office of Financial Research was created. According to the Treasury, the mission is to "improve the quality of financial data available to policymakers, and facilitate more robust and sophisticated analysis of the financial system." If this new office is going to be tasked with gathering significant financial information from across the Nation, are we creating a very fertile ground and huge target for hackers, in your opinion? Dr. Shannon?

Mr. SHANNON. Thank you.

There are many targets already out there. As we have heard in the testimony, there are many sources for hackers to attack. Clearly, an aggregated collection of data offers potentially even more of a target, but what should be considered is what is the right information to put into that. You don't need to have a fishing expedition in terms of collecting anything and everything, but clearly, a certain level of fidelity about cases, if you are trying to get an overall situation awareness, is important. On the other hand, if you are trying to use it for oversight of specific organizations or individuals, that is a different animal.

Chairwoman CAPITO. So what I am hearing you saying is there are all kinds of other opportunities out there, so this one particular one doesn't create a new and better opportunity. Am I hearing you correctly?

Mr. SHANNON. Correct. There are lots of good opportunities, and in various sectors they are creating other opportunities, if you will, but using the right security protections won't be the issue. It will be probably more of some of the privacy issue.

Mr. ROTENBERG. I actually do share your concern. I am not familiar with the specific provisions of the legislation. I think general reporting requirements are important and useful, but the collection of sensitive data can create new risks, and we have recommended, for example, techniques to anonymize or de-identify or minimize data collection so as to reduce those risks. So I think there is a way to do it, but I think it has to be done with some sensitivity about the data that is being collected.

Chairwoman CAPITO. Okay. Now, let me ask you, Mr. Nelson's organization, I have just established that Bank of America is one of your members. Is Verizon one of your members?

Mr. NELSON. No. We are just financial services organizations, but they have been a sponsor of ours in the past, and Symantec.

Chairwoman CAPITO. I am drumming up your membership here. And then do you share your data with—and I think you said this in your testimony—with the FBI, the folks we saw in panel one? Is there really a coordination between the private sector and the government sector and law enforcement that—and I am not disputing their testimony, I certainly thought it was excellent, but would you corroborate that testimony?

Mr. NELSON. Yes. I think it really kicked off in 2009. I remember being summoned by the FBI—and I don't know when—if you have ever been summoned by the FBI and not given a reason why, I was a little worried. But I showed up, and I was in a room with about 20 agents. I think Gordon Snow was there, his other deputies were there, and they described this situation, and it was this commercial account takeover situation. And they said, we knew about commercial account takeover, but we didn't realize it had become an epidemic. They had 85 cases they were investigating. They were adding 10 a week, and they said, we need to get something out to the industry. We don't want to compromise our investigations, but we need you, the FS-ISAC, to help us with this.

And I brought NACHA in, which is the rulemaking body for the ACH network, because mostly these involved ACH transactions. The losses were pretty high. Businesses were affected, school districts, municipalities. We ended up—what we used to tell people when they got attacked, we told banks to tell their customers, is don't click on that link. That wasn't good enough. So we spent 3 weeks—our threat intelligence committee volunteers—working with the FBI, working with NACHA's legal staff, and came up with a whole series of pretty in-depth layer defense recommendations. Those become the basis really for FFIEC supplemental guidance in June. So I think that cooperation was pretty obvious.

In July and August, I gave three different presentations to bank regulating groups that were having conferences at the FDIC, where I spoke to over 500 bank regulators about what we are doing, but also about what they have to do in terms of their own guidance. So I think the cooperation has been there.

In terms of actual information-sharing and operational information-sharing—

Chairwoman CAPITO. I am kind of at the end of my time here.

Mr. NELSON. Never mind.

Chairwoman CAPITO. Okay.

Mrs. Maloney.

Mrs. MALONEY. I thank all of you for your hard work and your testimony today.

After 9/11, we created across this country, or the law enforcement did, antiterrorism task forces on the local level to react and share information. The prior panel said that there were 24 task forces created in our country now on a regional level to share information. So I would like to ask first Mr. Garcia, or anyone on the panel, if any of you are participating in these tasks forces that they mentioned, and how do they work? Are they working?

So Mr. Garcia first, and anyone else who may be participating. I assume you are from New York. New York has to have one of these task forces, and I would like to hear your comments on it.

Mr. GARCIA. That is a very good question. Thank you for asking it.

What was referred to at that time, I believe, was the Secret Service, which sponsors the Electronic Crimes Task Force. We have Bank of America associates who participate in those forums where they gather with government and industry representatives to discuss threats, vulnerabilities, and best practices.

The FBI, similarly, has a program called InfraGard with chapters all over the country, including in New York, where the same type of activity happens. So this is all for the good where we have law enforcement, government agencies, and the private sector sharing what they know.

Greg Schaffer also alluded to the National Communications and Cyber Integration Center, the NCCIC, which is a 24-by-7 watch and warning center located in Arlington, hosted by DHS. The FS-ISAC has a seat on the NCCIC, and it is a watch floor with government agencies and private sector, including information technology and communications, the people who are sharing information real-time about what is happening on their networks, how are we responding to it, where is it coming from, what is the method, and what do we do about it, and we do it jointly.

So I think the partnership framework is getting more and more mature every year, and it can only get better from here. And Bank of America is very actively engaged in as many partnerships as we can to get better for ourselves and to help the broader ecosystem.

Mrs. MALONEY. You mentioned the Secret Service had their task force, the FBI had their task force. Would it be a better model if you followed what the intelligence system is doing in our country and have the task forces integrating everyone in the same room from the local up to the top, in your opinion?

Mr. GARCIA. I believe that is really the mission and objective of the NCCIC, the National Cyber and Communications Integration Center, at DHS, and it is just getting started, and it is getting developed with more members, more standards of practice, and I think it is maturing very well.

Mrs. MALONEY. I did want to comment on Mr. Rotenberg's comments that we do need to protect the privacy, and that we need to take steps in that direction.

I would like to ask the panel, even though it is not a legislative one today, a group of legislative proposals were put forward by the Administration in this area. I would like to ask you, have you read

it? Are you aware of it? Are there any proposals that you think are particularly worthy?

Mr. SHANNON. I will just make one simple comment here. The safe harbor provisions for sharing data so that organizations and individuals can do the right thing, as they are responding, time is usually of the essence in many of these incidences, especially national security ones, and safe harbor-type provisions, I think, enable people to do that right thing, and we certainly support that.

Mr. TILLETT. I would like to add to that the actionable intelligence that needs to be shared. We have a number of different public-private relationships which are sharing this information. So actionable intelligence and real-time intelligence is of high importance on this, but I think often what we see is we don't need to reinvent the wheel. We just need to make it work better, we need to speak a common language. And I think that those initiatives are in process amongst many of these private-public relationships, but we absolutely need to embrace and endorse that so we are not speaking past each other and we are not speaking above each other. We all understand a common language about the current threat.

Mrs. MALONEY. In terms of technology, do you think any foreign country has superior technology in this whole form of hacking and protection, or are we leading the way in this area? What is your opinion, anyone?

Mr. SHANNON. As mentioned in the data breach report, a lot of the at-scale for these cybercriminals, it is using fairly simple techniques. But I believe in other venues, the specific capabilities can be addressed, but they haven't taken us down significantly yet. So I see that as a good sign. The stock market operates, the press operates—

Mrs. MALONEY. And they have to now talk about a cyberattack that would stop our communications—yes, Mr. Sartin?

Mr. SARTIN. I was just going to add to that about the international perspective. We do see variances in knowledge about security, implementation. We see variances in the technologies that are adopted from one country to the next, generally whether it is the people who process the technology, the combination of that. I don't necessarily see that one country is necessarily better prepared than any other. It comes down to individual data breach victims.

Mrs. MALONEY. Thank you. My time has expired. It has been very insightful. Thank you for your hard work, all of you, and your presentation today. Thank you.

Chairwoman CAPITO. Thank you.

I have one additional question for Mr. Nelson regarding notification of breaches and other cyber crimes. I understand there is an update to FinCEN's suspicious activity report form. Do you think this will help law enforcement better understand the cyberthreat?

Mr. NELSON. Yes. I think today it is not really identified. FinCEN's commercial account takeover is—you don't have a box you can check on the form today to indicate what that is. I think we could actually have a better idea—in my report, I have some information about a survey we did, and 77 institutions responded, but that is not the whole industry. So if SARs reports could indicate those types of attack, the different types of attacks, what the

losses actually were, we would have a better understanding what the losses were and the losses that were prevented. In many cases, the losses—funds don't go out the door, or if they do, the receiving institution returns the money.

Chairwoman CAPITO. I, too, want to thank all of the witnesses, and I have to say one last thing myself. From an individual standpoint, I think we have to be patient as Americans to realize that there are a lot of people out there trying to protect our financial information, our personal information, and when we receive, like we all have, those phone calls where we will try to use your card or whatever, and you are locked out, we have a tendency to lose our patience and become very frustrated, and many times these efforts are going forward to try to protect us as individuals and us as families.

And I don't know that my statement is going to do any good towards that. Maybe I am talking to myself here a little bit, but I think we all need to remind ourselves that it is not quite as simple as it looks. It is not as easy as it looks to reach into your pocket, and you forget about all the infrastructure that is going on behind you.

This concludes our hearing. The Chair notes that some members may have additional questions for this panel which they may wish to submit in writing. Without objection, the hearing record will remain open for 30 days for members to submit written questions to these witnesses and to place their responses in the record.

I appreciate you all very much for coming in, and we are very interested in the topic. And with that, the hearing is adjourned.

[Whereupon, at 12:48 p.m., the hearing was adjourned.]

A P P E N D I X

September 14, 2011

TESTIMONY OF

GREG GARCIA

PARTNERSHIP EXECUTIVE
for
CYBERSECURITY AND IDENTITY MANAGEMENT

BANK OF AMERICA

Before the

HOUSE FINANCIAL SERVICES

FINANCIAL INSTITUTIONS AND CONSUMER CREDIT SUBCOMMITTEE

WASHINGTON, DC

SEPTEMBER 14, 2011

Introduction

Chairman Capito, Ranking Member Maloney, and distinguished Members of the Committee, I am Greg Garcia, Partnership Executive for Cybersecurity and Identity Management within Bank of America's Global Technology & Operations (GT&O) organization. Thank you for inviting us to share our approach to cyber security challenges facing our bank and the financial sector as a whole. My role is to coordinate Bank of America's external public private partnerships as they relate to cybersecurity and identity management so that we ensure a coherent strategy, better operationalize what we learn in the broader community, and maximize our contributions to the security of the cyber ecosystem to reduce overall risk.

Bank of America is one of the world's largest financial institutions, serving individual consumers, small- and middle-market businesses and large corporations with a full range of banking, investing, asset management and other financial and risk management products and services. The company provides unmatched convenience in the United States, serving approximately 58 million consumer and small business relationships with approximately 5,700 retail banking offices and approximately 17,800 ATMs and award-winning online banking with 30 million active users. Bank of America is among the world's leading wealth management companies and is a global leader in corporate and investment banking and trading across a broad range of asset classes, serving corporations, governments, institutions and individuals around the world. Bank of America offers industry-leading support to approximately 4 million small business owners through a suite of innovative, easy-to-use online products and services. The company serves clients through operations in more than 40 countries.

My background and contributions in cybersecurity over the past decade complement Bank of America's proactive and aggressive strategy. I was honored to have served as the nation's first Assistant Secretary for Cyber Security and Communications at the U.S. Department of Homeland Security from 2006-2008. I also had the privilege of serving as a staff member of the House Science Committee from 2001-2003 where I assisted Chairman Sherwood Boehlert in shepherding enactment of the Cyber Security Research and Development Act of 2002. Other cyber security partnership and policy roles on behalf of the technology sector have given me a unique cross-sectoral view of the challenges and opportunities from both an industry and government perspective.

We commend the committee for holding this hearing today to discuss the important issue of cybersecurity. My testimony will provide an overview of the current cybersecurity threat environment; how Bank of America manages security to protect its enterprise, customers, and shareholders; and how we partner with the rest of the financial sector, other industry sectors and the government to mitigate the risks associated with those threats.

Overview of the Threat Environment

The global financial system operates on a vast network of information and communications technology, both wired and wireless. Trillions of dollars in transactions per day flow across this network globally, from online banking and deposits, loans and credit card payments, large commercial transactions, to making payroll, raising capital and issuing debt, and securities trading, among many other services. It is our responsibility to ensure the smooth and uninterrupted delivery of those services wherever we do business around the world and to secure the data and networks that enable them and prevent unauthorized access that could lead to fraud, identity theft, data loss, or system downtime. Bank of

America's information technology infrastructure not only enables the provision of financial services, but it also guards, defends and protects those services and the data our customers entrust to Bank of America. Cyber access and the potential to disrupt these flows make the financial sector a target in the context of all threats.

It is important to note that while motivations for cyber attack differ, many of their techniques are the same, but at different levels of sophistication. We see "joy-riding", in which individuals simply want to make mischief; there are cyber criminals and criminal rings that are in it for the money, whether dealing in the credit card black market, account takeover schemes, fraudulent payments or ATM "skimming"; and there are more sophisticated threats from well organized "hacktivists" and nation states motivated to steal sensitive, strategic, or intellectual property information, disrupt services, deface websites and cause fear, loss of confidence and reputational damage.

While our emphasis has been primarily on the middle spectrum of threats – to protect our customers from fraud and identity theft, over the past few years there has been an emerging threat of greater sophistication and stealth that keeps us on alert 24x7x365.

How Bank of America Addresses the Cyber Threat

At Bank of America we are laser focused on cybersecurity. In discussing how we manage cyber security, it is useful to break it down into two interrelated components: our customer facing policies and activities, and our enterprise security.

Customer Security

Of primary importance to us is securing our customer financial information, and we deliver a range of services to secure transactions and keep our consumer customers whole. For example:

ShopSafe®
A free service that lets customers shop online without sharing their real credit number. Each time an online purchase is made, ShopSafe conveniently creates a temporary card number.

Fraud monitoring
Total Security Protection is free and automatically offered on Bank of America consumer credit and debit cards. It monitors how and where customer cards are being used. Our security systems analyze millions of transactions a day looking for patterns to help identify and stop fraud and identity theft.

Identity theft assistance
Bank of America is committed to helping victims of identity theft. We also offer the services of ITAC (Identity Theft Assistance Center) to help with identity theft recovery, prevention and education.

#1-rated safety features
Our customer safety features have ranked #1 for 5 years in a row by Javelin Strategy & Research, the nation's leading provider of research on financial institutions.

$0 Liability Guarantee
Should any unauthorized purchases originate from Online Banking, we reimburse customer losses when reported within a reasonable time.

Secure technology
Our fraud prevention and security systems protect customers with the latest encryption technology and secured email communication.

We also offer our customers many tips online about what they can do to protect themselves. In particular, "phishing" remains one of the most widely used and effective attack methods by cyber criminals and hackers. Targeted emails that look legitimate but trick receivers into clicking on malicious links or entering personal information are difficult to prevent, and consumers, small businesses, large businesses and governments, are all at risk and must take appropriate precautions through awareness, training, up-to-date technology and strong security practices.

Enterprise Security

Our customer facing security strength relies on many of the policies and capabilities that protect and enable our broader enterprise. And at an enterprise level, we are concerned not just for our customers and employees, but for the protection of critical, nonpublic data, intellectual property, and operational availability and continuity. It is in all of these areas that we work very closely with our regulators to ensure we apply, maintain and constantly measure all the necessary security controls across the enterprise.

Fundamentally, our cybersecurity program is based on a combination of people, process and technology.

Across the company, all of our employees receive annual training on the importance of information protection, the policies and methods the bank uses, and the responsibilities of every user.

We have an information security team of advanced technology experts who have past careers in law enforcement, the military, security and high technology innovation. And we're constantly looking to increase the pipeline of new talent.

We operate under detailed, rigorous information security policies, with a program designed to protect the security and confidentiality of customer and client information, from acquisition to use and storage to disposal.

Finally, we invest in and deploy leading-edge technology to secure data in movement and at rest. Where specific technology needs are not available off the shelf we often design and implement our own. Bank of America holds at least 140 patents in security technology so that we can deploy tools that meet our often unique requirements in a highly scalable way.

In addition, our security policy has the support and attention at the highest levels of the company. Bank of America's Board of Directors approves the bank's information security policy and programs, and the board is kept informed on the overall status of our information security program.

Our information security program is also subject to ongoing regulatory oversight and examination. Each of our business and support units has an executive accountable for information security, and a team of experienced associates to help implement policies, standards and baselines.

Increasing Our Investment

As an enterprise strategy, our security framework is organized along the 5 pillars of a structured cyber security operating model: Our goal is to: Deter, Prevent, Protect, Respond and Recover.

To describe each one briefly:

> **Deter**: Discourage attacks through improved treaties, laws and increased enforcement
> **Prevent**: Reduce incidents by better anticipating threats and addressing critical vulnerabilities
> **Protect**: Protect our business systems through integrated controls across the stack: access, applications, information and infrastructure
> **Respond**: Mitigate incidents through a proactive monitoring and agile incident response capability
> **Recover**: Conduct forensics on events, work with investigations, and capture lessons learned to improve our security posture

We are investing heavily in developing a progressive standard of practice across those 5 pillars that is commensurate with the financial industry's status as critical national infrastructure. We believe that as companies across the financial sector and other critical sectors adopt the same structured methodology for managing against the sophisticated and evolving range of threats we face, we will collectively be able to stay ahead of the cyber criminals, hackers and other adversaries.

Partnership is Key to Cybersecurity Management

A critical element of a mature cyber security program is an investment in partnerships and collaboration. A mature partnership program can contribute outcomes to all elements of "people, process and technology" as well as the five pillars of a cybersecurity operating model, both within the walls of the company and externally for the broader good of the community. At Bank of America, we are bolstering our partnerships and collaboration to gain the broadest view of the threat landscape and innovative solutions, and we are sharing information and best practices so that we can collectively get smarter and better at protecting assets and critical information.

For example, among many others, we are coordinating and supporting partnerships such as the Financial Services Sector Coordinating Council, the Financial Services Information Sharing and Analysis Center (FS-ISAC), the Department of Homeland Security's cybersecurity entities and law enforcement partners globally. We consider these partnerships within the sector and across the cyber ecosystem to be essential elements of our ability to protect our customers, investors and shareholders from fraud, identity theft, cyber attack and business disruption. We treat every partnership as an opportunity to either improve our own internal security capabilities or an opportunity to extend our expertise and situational awareness to other partners.

The bottom line is: No one entity has all the information; it takes teamwork to bring all the pieces together to complete the picture.

Development of the Critical Infrastructure Partnership Model

This model of partnership has its official roots in a 2003 presidential directive – Homeland Security Presidential Directive (HSPD) 7. HSPD 7 set forth the imperative that "critical infrastructure" industry sectors are strongly encouraged to self-organize around a mission to identify and measure cyber and physical threats and vulnerabilities across the sector and work together with interdependent stakeholders such as other industries and government to mitigate those vulnerabilities.

HSPD 7 established a structure – now known as the National Infrastructure Protection Plan, or "NIPP" - that assigned sector specific agencies or "SSA's" to each organized sector to work in partnership to address current and emerging issues. In the case of financial services and the Financial Services Sector Coordinating Council which is described below, the U.S. Department of Treasury is the assigned SSA.

In addition to these more formal public private partnerships, Bank of America participates actively in a large number of other industry to industry, company to company, and company to government efforts to quite simply get better at what we do – to exchange actionable intelligence, to adopt and share best practices, and to develop longer-term policy and strategic approaches to collectively strengthen the security of the ecosystem in which we all operate. This program is well founded on the understanding that we are all interconnected, interdependent and in this together.

The following summarize just a few of the many collaborations and initiatives that Bank of America contributes to and leverages to bolster our security posture and that of the broader ecosystem:

Industry to Government

Financial Services Sector Coordinating Council (FSSCC)
The Financial Services Sector Coordinating Council is a group of more than 45 private-sector firms and financial trade associations that reinforces the financial sector's resilience against threats and all hazards to the nation's financial infrastructure. Formed in 2002, FSSCC works with the Department of Treasury, which has direct responsibility for infrastructure protection and homeland security efforts for the financial services sector, while also serving under the overall guidance of the Department for Homeland Security.

I serve as co-chair of the FSSCC Cyber Security Committee where, among other activities, we are leading the effort to develop a financial sector annex to the National Cyber Incident Response Plan so that we have a uniform and coherent set of procedures for aligning sector-wide and national response to a cyber incident of significant impact.

For additional detail on the FSSCC's perspective on cybersecurity, I refer the Committee to the April 15, 2011 testimony of FSSCC Chair Jane Carlin before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Homeland Security Committee.

Financial Services Information Sharing and Analysis Center (FS-ISAC)
The industry forum for collaboration on critical security threats facing the financial services sector. Bank of America serves on the FS-ISAC Board of Directors and its Threat Intelligence Committee.

Taken together, the FSSCC and the FS-ISAC serve as the primary financial industry policy and operational components under the NIPP partnership model. Both the FSSCC and the FS-ISAC maintain

a strategic role through information sharing and collaboration among stakeholders (e.g., Federal agencies infrastructure providers, and other financial services firms), education and awareness, preparedness planning, issuance of guidelines/ good practices, and developing mitigation/protection strategies against threats, incidents, and vulnerabilities. The FSSCC and FS-ISAC also maintain a cross sector coordination role based on established relationships. In this capacity, they are responsible for mobilizing interaction with critical external partners and agencies to support accurate situational awareness and resource support requirements (to and from the FS Sector and its constituents).

Financial and Banking Information Infrastructure Committee (FBIIC)
As the government partner to the FSSCC, the FBIIC is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public-private partnership. Treasury's Assistant Secretary for Financial Institutions chairs the committee. The FSSCC and FBIIC hold a joint meeting semi-annually.

National Cyber Forensics Training Academy (NCFTA)
The NCFTA functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime. Bank of America is deploying bank personnel to serve on the NCFTA on a rotational basis.

National Cybersecurity and Communications Integration Center (NCCIC) and the Unified Coordination Group (UCG)
The NCCIC provides an integrated incident response facility to mitigate risks that could disrupt or degrade critical information technology functions and services, while allowing for flexibility in handling traditional voice and more modern data networks. The NCCIC was created at the recommendation of the National Security Telecommunications Advisory Committee, the Government Accountability Office and a joint industry-government working group, which together emphasized the need for collocation, integration, and interoperability among existing cyber and communications incident response mechanisms. Bank of America and the financial sector are represented on the NCCIC watch floor by the FS-ISAC.
Cyber UCG
The Cyber UCG is an interagency and inter-organizational body that incorporates public and private sector officials ensuring unity of coordination and the facilitation of rapid collaboration in response to cyber events of national significance. It has roles and responsibilities during steady state and cyber incidents under the National Cyber Incident Response Plan. As co-chair of the FSSCC Cyber Secrity Committee, I serve on the UCG.

Department of Homeland Security U.S. Computer Emergency Readiness Team (US-CERT)
US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinates cyber information sharing, and proactively manages cyber risks to the Nation while protecting the constitutional rights of Americans. Bank of America, the FS-ISAC and many financial institutions exchange information with US-CERT on an ongoing basis, and the relationship is maturing.

Cross Sector Cyber Security Working Group
The Cross-Sector Cybersecurity Working Group (CSCSWG), founded by the Department of Homeland Security, serves as a forum to bring government and the private sector together to collaboratively address risk across the critical infrastructure sectors. This cross-sector perspective facilitates the sharing of perspectives and knowledge about various cybersecurity concerns, such as common vulnerabilities

and protective measures, and leverages functional cyber expertise in a comprehensive forum. Bank of America serves as the financial services representative to the CSCSWG.

Government Information Sharing Framework (GISF)
The GISF is an information sharing agreement between FS-ISAC, DHS and the Department of Defense for the purpose of sharing timely, accurate, and actionable warnings of physical, operational, and cyber threats or attacks on the national financial services infrastructure.

Electronic Crimes Task Force
The ECTF network brings together federal, state and local law enforcement, as well as prosecutors, private industry and academia, for common purpose of prevention, detection, mitigation and aggressive investigation of attacks on our nation's financial and critical infrastructures. Bank of America associates participate in various ECTF events across the country throughout the year.

InfraGard
InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Bank of America associates are members of and participate in various InfraGard events across the country throughout the year.

Industry to Industry

Bank of America Cyber Collaboration Program
Bank of America actively seeks out other like-minded companies that similarly find value in establishing more intimate and trusted information sharing relationships to exchange data on threats, vulnerabilities, incidents and response efforts. We have nearly 2 dozen individual partnerships with companies from within the sector and outside the sector. These more informal relationships help us not only get better and smarter now, but the fact that we are exchanging business cards now rather than when an incident occurs means we have already established a level of preparedness that could not have been achieved in isolation. The benefits from these partnerships just in the past 12 months have yielded measurable results in dollar value and improved situational awareness and preparedness.

BITS
A division of the Financial Services Roundtable, BITS was formed in 1996 by the CEOs of member institutions to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS works to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. Bank of America serves on the Executive and Advisory Boards of BITS as well on its as numerous subject matter working groups.

Identity Theft Assistance Center
ITAC, the Identity Theft Assistance Center, is the leading consumer advocate on identity fraud and the financial services industry's identity management solution center. An affiliate of The Financial Services Roundtable, ITAC is supported by the industry as a free service for our customers. Since 2004, ITAC has helped tens of thousands of consumers restore their identity. Bank of America has served on the ITAC Board and as its chair.

National Cyber Security Alliance

NCSA's mission is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets. Bank of America serves on the board of NCSA.

Cyber Campaigns

Participation in Cyber Exercises and Crisis Playbooks
Bank of America has participated in multiple financial services exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of lessons learned. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the 2009 Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) exercise were jointly executed by the FSSCC, FS-ISAC, and included many FBIIC members, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), DHS, and more than 800 individual participants. Members of the FSSCC are also planning to participate later this fall in an exercise of our ability as a sector to respond to a cyber incident of national significance, testing the Financial Services annex (currently in development) to the National Cyber Incident Response Plan.

National Cyber Security Awareness Month
National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, is an annual awareness-raising effort that seeks to encourage everyone to protect their networks and our nation's critical cyber infrastructure. Bank of America supports NCSAM with activities and messaging aimed internally at employees and at our millions of customers and all consumers to raise awareness about how we protect information and assets and what every individual can do to protect their own corner of cyberspace. Central to the theme is that cyber security is a shared challenge and a shared responsibility.

Stop.Think.Connect
The Stop.Think.Connect. (STC) Campaign launched in October 2010 in conjunction with National Cybersecurity Awareness Month. STC is part of a public awareness campaign effort among Federal and State governments, industry, and non-profit organizations to promote safe online behavior and practices.

National Initiative for Cybersecurity Education (NICE)
Launched by the Obama Administration last year, NICE is a national campaign to promote cybersecurity awareness and digital literacy across industry, government and academia, and to build a digital workforce for the 21st century. Bank of America supports this effort and is exploring opportunities to contribute.

Conclusion

In conclusion Chairwoman Capito, I am proud to say that Bank of America is focusing a tremendous amount of resources and energy to staying ahead of the cyber security challenge. We have come a long way as an institution and as a sector. We are developing new tools, processes and expertise for meeting the challenge of cyber crime. We are making the necessary investments and taking our regulatory compliance obligations seriously, just as we are working proactively to do more than is required by regulation. Our ultimate goal is protect our customers, our shareholders, and our enterprise.

We also have seen our working relationships with government and industry partners evolve and mature for the good in partnership initiatives that are not subject to – indeed cannot be effectively subject to – regulatory compliance. While we recognize the importance of uniform regulatory standards to set a minimum bar across the sector and hold us accountable, we also recognize that the evolving nature of cybercrime requires a resilient and evolving partnership structure that is responsive and adaptable in the kind of real time dynamic that a regulatory structure is insufficient to ensure.

But of course, this is not to say we are where we need to be. We have more work to do. We are constantly seeking ways to build trust relationships and information sharing partnerships with government that transcend concerns about secret-level classification and business sensitive information. Most acknowledge that actionable threat information that is not shared is useless information. The more we develop and populate those institutional structures such as the FS-ISAC, FSSCC, the NCCIC and others, that are designed to facilitate broad situational awareness, a common operational picture, best practices and real-time incident response, the better and more secure will be our financial infrastructure, our economy and the homeland.

Final Recommendations

As mentioned earlier, we have much to do, both in industry and in government. Let me close by making a few recommendations for additional measures we can take together:

Government can:

- Enact stronger laws against hacking with continued enhancement of enforcement capabilities
- Prioritize long-term, basic research into cyber "grand challenges" not typically undertaken by the private sector
- Simplify and streamline multiple, simultaneous and sometimes conflicting government efforts to "solve" the problem

We all can:

- Urge and support industry efforts to take cyber responsibility within the current critical infrastructure partnership structure
- Better share technology and R&D between the private sector and government labs
- Invest more in education, training and awareness
- Develop more collaborative operations and open channels for faster, better information sharing and actionable intelligence
- Increase coordination internationally
- Continue to build consumer awareness

Madam Chairman, that concludes my testimony. Thank you.

Testimony of

William B. Nelson

On Behalf of the

The Financial Services Information Sharing & Analysis Center

Before the

United States House of Representatives

Financial Institutions and Consumer Credit Subcommittee

September 14, 2011

FS-ISAC BACKGROUND

Chairman Capito, Ranking Member Maloney, and members of the Subcommittee, my name is William B. Nelson. I am President and CEO of the Financial Services Information Sharing & Analysis Center (FS-ISAC). I want to thank you for this opportunity to address the U.S. House of Representatives Financial Institutions and Consumer Credit Subcommittee on the important issue of cyber crime, its impact to the financial services industry, and the cooperation and information sharing between government agencies and the private sector.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD63) that called for the public and private sector to work together to address cyber threats to the Nation's critical infrastructures. After 9/11, and in response Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to over 4,200 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 30 trade associations representing the majority of the U.S. financial services sector.

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and state and local governments.

With respect to cooperation within the financial services sector, the FS-ISAC is a member of, and partner to the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection established under HSPD7. We also work closely with other industry groups and trade associations that are members of the FS-ISAC including the American Bankers Association (ABA), Securities Industry and Financial Markets Association (SIFMA), Independent Community Bankers Association (ICBA), and the BITS division of the Financial Services Roundtable. In addition, our membership includes various payments, clearing houses and exchanges such as the National Automated Clearing House Association (NACHA), Depository Trust and Clearing Corporation (DTCC), New York Stock Exchange, NASDAQ, The Clearing House (TCH), the various payment card brands and most of the card payment processors in the U.S.

The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so information that would normally not be shared is able to be provided from the

originator and shared for the good of the sector, the membership and the nation. A complete list of FS-ISAC information sharing services and activities include:

- delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the 24x7x365 FS-ISAC Security Operations Center (SOC);
- an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner preparing cyber security briefings and white papers;
- operation of email list servers supporting attributable information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;
- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;

- development of risk mitigation best practices, threat viewpoints and toolkits;
- Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee that provide in-depth analyses of risks to the sector, provide technical, business and operational impact assessments and recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force (see pages 11 - 16);
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;
- semi-annual member meetings and conferences; and
- online webinar presentations and regional outreach programs to educate small to medium sized regional financial services firms on threats, risks and best practices.

A key factor in all of these activities is trust. The FS-ISAC works to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies.

The FS-ISAC has implemented a number of programs in partnership with the Department of Homeland Security (DHS) and other government agencies. Earlier this year, the FS-ISAC, in partnership with DHS became the third ISAC to participate in the National Cybersecurity and

Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. While this program is relatively new, our presence on the NCIC floor has largely greatly enhanced situational awareness and information sharing between the financial services sector and the government.

As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in near real-time. This listserv allow FS-ISAC members to share directly with U.S. CERT and further facilitates the information sharing that is already occurring between FS-ISAC members and with the NCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's handling and communications with various sectors following the RSA attack in March of this year is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, it should be noted that the FS-ISAC and FSSCC have worked closely with DHS, the U.S. Department of Treasury, FBI, U.S Secret Service and other government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information

security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

PUBLIC / PRIVATE SECTOR RESPONSE TO THE CYBER CRIME ISSUE

The FS-ISAC is aware through its information sharing arrangements with both public and private sector organizations that criminal threats are targeting US financial institutions, capital markets exchanges, clearing houses, payment processors, businesses and consumers. However, research shows that losses due to cyber crime currently only account for a small percentage of the overall fraud losses incurred by financial institutions. In the last eighteen months, actual losses experienced by financial institutions and their customers as a result of cyber-related fraud has actually declined in spite of the fact that the number of attacks has increased. The FS-ISAC and its members recognize the online criminal threat both to the affected institutions and to consumer confidence posed by these criminal activities and we are taking steps to address areas of concern.

Law enforcement and a number of government agencies have taken a lead role working with the FS-ISAC, its member organizations, payments processors, and the financial services sector as a whole to combat these types of attacks. An example of a successful instance of government/financial services sector information sharing occurred on August 24, 2009, when the FBI, FS-ISAC and NACHA released a joint bulletin concerning account takeover activities targeting business and corporate customers. The bulletin described the methods and tools employed in recent fraud activities perpetrated against small to medium-size businesses that had

been reported to the FBI. The objective of the bulletin was to employ FS-ISAC and NACHA subject matter expertise and apply it to the FBI case information to identify detailed threat detection, prevention, and risk mitigation strategies for financial institutions and their business customers, whilst preserving the integrity of the FBI's ongoing investigations. The FS-ISAC and NACHA developed a comprehensive list of recommendations for financial institutions to educate their business customers on the need to use online banking services in a secure manner. The bulletin was distributed through the FS-ISAC to its over 4,200 members, which includes over 30 member associations such as NACHA, ABA, and ICBA. Subsequent releases of the bulletin were shared with the press in 2010, redacting sensitive information about the ongoing investigations.

The risk mitigation tactics that are outlined in the joint FBI/FS-ISAC/NACHA bulletin include information security best practices that are consistent with the 2005 Federal Financial Institutions Examination Council's (FFIEC's) Guidance on Authentication in an Internet Banking Environment. The joint FBI/FS-ISAC/NACHA bulletin actually moved further than the 2005 FFIEC Guidance in its recommendations. Specifically, the bulletin recommended that financial institutions implement a layered "defense in-depth" approach to information security to protect financial institutions and their customers.

FFIEC SUPPLEMENTAL GUIDANCE ON INTERNET BANKING AUTHENTICATION

The recent FFIEC Supplemental Guidance on Internet Banking Authentication released on June 28, 2011 incorporates many "defense in-depth" recommendations and include a number of very

important new regulatory provisions. The following is a summary of some of the Supplemental Guidance's key provisions.

The Guidance reinforces existing supervisory expectations for annual risk assessments by financial institutions. These risk assessments should consider changes in the internal/external threat environment, changes in the financial institution's customer base, changes in functionality to online Internet services, and the financial institution's actual fraud experiences. Authentication controls should be upgraded in response to risk assessments.

For the first time, the FFIEC distinguishes between retail and commercial accounts. It raises the bar for minimum controls for all accounts and recognizes that commercial accounts pose a higher level of risk. Commercial account controls should be consistent with increased levels of risk and stronger than controls for consumer accounts.

The FFIEC Supplemental Guidance now requires financial institutions to have layered security for consumer accounts. "Layered security" is defined as having different controls at different points in a process, so that weakness in one control is compensated by strengths in another control. At a minimum, layered security should include anomaly detection and response at initial customer login, and at initiation of funds transfers to other parties. Layered security for commercial accounts should be stronger than those implemented for consumer accounts. The Guidance specifies enhanced controls for system administrators of commercial accounts. Examples of these enhanced controls include additional authentication/verification of new payees and changes to established value threshold or time windows.

Layered security should now include anomaly detection. Changes in consumer or commercial account activity should be detected and steps taken to ensure that additional controls are in place if such activity is discovered. However, according to the FFIEC Supplemental Guidance, "simple" device identification and challenge questions are no longer deemed effective as a primary control. Instead, financial institutions will be required to implement "*Complex Device Identification.*" An example of complex device ID includes use of a one-time cookie, in conjunction with other factors such as the PC's configuration, IP address, and geo-location used to create a digital "fingerprint" of the customer's personal computer. The Guidance also calls for more "*Complex Challenge Questions*" not easily found by cyber criminals on the Internet. These "out of wallet" questions should not rely on publicly available information and there should be more than one question, potentially even including a "red herring" question that only the account holder will recognize as false requiring a potentially fabricated answer.

Lastly, the FFIEC Supplemental Guidance calls for increased customer awareness/education efforts by financial institutions. The Guidance recognizes that customers have an important role to play in online banking security and that for consumers and small businesses, their financial institution is most likely the more knowledgeable party concerning online security. Financial institutions have an obligation to help customers practice good online banking security and clarify consumer rights under Regulation E. Financial institutions should also educate their commercial account holders, especially small businesses, on use of security controls that are available for their online banking services.

FFIEC regulatory agencies will begin examinations in January 2012 to assess conformance with the new FFIEC Supplemental Guidance.

FS-ISAC ACCOUNT TAKEOVER TASK FORCE

In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies.

The ATOTF has focused on deliverables in three areas of effective cyber defense: Prevention, Detection and Response. Deliverables for each of these subgroups include:

1. Prevention

- Industry Advisories
  - Corporate & Small Business Customers
    - Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3) The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf
  - Financial Institutions
  - Retail Customers & Consumers

    - Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
    - Example of a Work-From-Home Scheme
  - J1-Visa Money Mule Advisory
  - Internet Auto Fraud

- Fraud Education and Awareness.

  Representatives and volunteers from the industry have participated in various financial services, regulatory, and corporate user events to educate the business and government community.

- Improve Information Sharing with Law Enforcement
  - Inventory information sharing portals
  - IP addresses involved in frauds, money mule accounts, attack signatures, Suspicious Activity Reports (SAR) and other fraud trends
  - First joint FBI/FS-ISAC Cyber Crime Report

- Develop Email Trust Relationship working with financial institutions and large Internet Service Providers (ISPs). The Trusted Email Registry is currently being piloted. Both BITS and FS-ISAC will announce to their members when it becomes available for general use, at which time both organizations will continue to encourage members to implement email authentication protocols.

2. Detection

- List of Vendors and Service Providers

  Smaller financial institutions use a core group of service providers and this list provide them with security offerings.

- Detection Whitepaper for financial institutions.
  - Document focused on detection of account takeover victims.
- Techniques for recovering customers from ZeuS or other keystroke logging/man-in-the-middle Trojan infections and the exploration of third-party services with the goal of gathering elements of intelligence to enable better detection methods.
- Development of Webinars and Training to enable better education of customers with the goal of aiding detection techniques while improving awareness of the issues.
- Document Standard Set of Requirements and enhancements for alerting and security requirements for core ACH/wire transfer software providers.

3. Response

- Contact List, Procedures

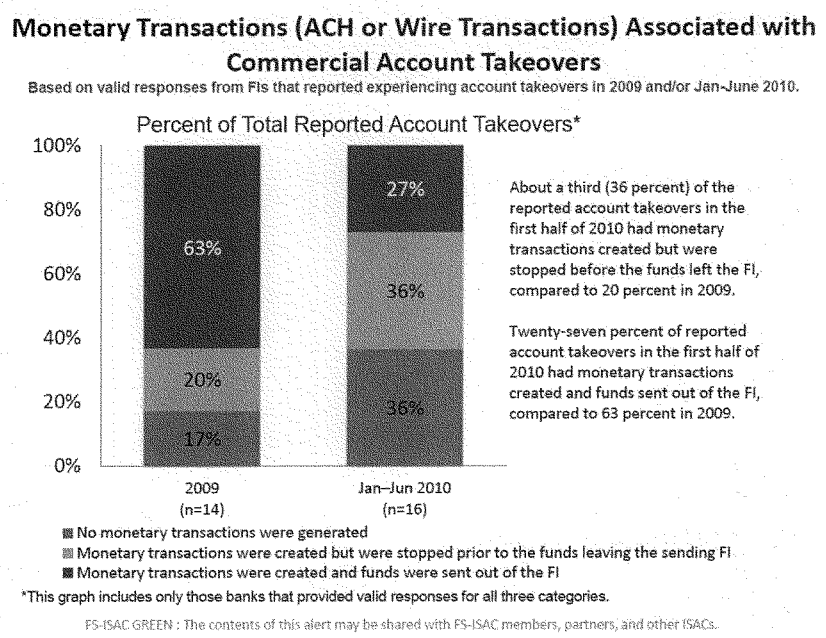
  This list provides financial institutions the information they need to report account takeover attacks via online banking to the Secret Service, FBI and other agencies, and a process for keeping the contact lists current.

- Form for Reporting account takeovers, including what should be submitted in the incident report and used for metrics to measure the success of the ATOTF.
- Actions financial institutions can take after an incident, communicated via FS-ISAC advisory notices.

- Monitor the National Cyber-Forensics & Training Alliance (NCFTA) Internet Fraud Alert service. This provides financial institutions with information for recovered credentials from the takedown of botnet command and control servers.
- List of forensic providers and forensic tool providers.
- List of Resources currently available for cyber crime and broad education so that financial institutions can leverage existing resources.
- Develop Malware Submission method and provide a process for sharing identified new malware with government/law enforcement agencies and anti-virus vendors.
- Redesign Suspicious Activity Report (SAR) Submission and Analysis Process by working with the Financial Crimes Enforcement Network (FinCEN) to give financial institutions and regulators more actionable information.
  - Recommendations for reporting an account take over attack via SARs.
- Add Fraud Contacts in FS-ISAC Membership Directory
  - FS-ISAC members updated contact information
- Conferences / Awareness—speeches by ATOTF members
  - May 2011 - Fiserv Risk Management Conference
  - June 2011 – The Clearing House Payments Forum
  - July 2011 - Advanced FFIEC Bank Secrecy Act / Anti-Money Laundering (BSA/AML) Specialists Conference
    - Continuing education to FFIEC examiners with specialized BSA/AML experience within the financial institution regulatory agencies.
    - Participants from OCC, FDIC, FBI, FS-ISAC
  - August 2011 - CERT's GFIRST conference

- August 2011 - International Association of Financial Crimes Investigators (IAFCI) conference
- August – FFIEC Bank Examination Conference
- FS-ISAC Account Takeover Workshops February to September 2011 – Twelve workshops conducted around the U.S. in cooperation with the Regional Payments Associations

- Baseline Account Take Over Survey
  - Establish baseline for Commercial Account Takeover attempts and losses for 2009 and the first half of 2010
  - 77 financial institutions responded to the survey
  - Statistics indicate financial institutions are doing a better job of stopping fraudulent transactions from being created and from funds leaving the financial institution
  - FS-ISAC will conduct another survey to capture data for all of 2010
    - Follow-up survey for 2011 data is also planned
  - The following chart illustrates one of the key findings of the Commercial Account Study (CAT). During the timeframe of the study, the trend shows that fewer monetary transactions are being created and if they are created, there are far less fraudulent payments leaving originating financial institutions.



As a result of the 2009 joint FBI/FS-ISAC/NACHA bulletin, the FFIEC Supplemental Guidance and the many deliverables of the ATOTF, financial services firms and their business, government, and consumer customers have become more aware of the online risks facing them and of the many effective layered defense practices to mitigate those risks. As a result, more financial institutions are now aware of how to detect, prevent and respond to malicious and criminal activities resulting from online attacks.

FS-ISAC EXERCISES

The FS-ISAC provides the 24x7x365 platform for its members to share information between themselves, with the government and law enforcement, and with other sectors. The FS-ISAC participates in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and provides support for FSSCC exercises such as CyberFIRE.

The FS-ISAC undertook on its own a major effort to conduct a national Cyber Attack Against Payment Processes (CAPP) Exercise in February 2010. The 2010 CAPP Exercise included a variety of simulated attacks that tested the financial services industry's ability to respond and react to different types of cyber attacks. The exercise provided a forum to raise awareness regarding best practices and remediation steps to minimize the risk to the financial services firms and their customers from these various types of attacks.

Participation in the exercise was not limited to FS-ISAC members. In addition to the 634 financial services firms that participated in the exercise, 67 business/government users of payments services, 34 payment processors and 29 retailers also participated in the three day event. The CAPP Exercise had several major findings in several key areas including the ability of firms to recognize and detect attacks, security policy, response and communication, preventing future attacks and a final set of recommendations. Further information about these findings can be found in the 2010 CAPP Exercise executive Summary published on this website: http://www.fsisac.com/files/public/db/p243.pdf

LAW ENFORCEMENT SUCCESSES

From a law enforcement perspective, recent progress has been made against some cyber crime activities. The Secret Service and the FBI have made numerous arrests in the last two years of many individuals and gangs responsible for various data breaches and criminal cyber attacks. These arrests have been important in stemming the tide of rising cyber attacks by going after the criminal masterminds behind them. Arrests have been made in many cases but some of the cyber criminals indicted operate in other countries, mostly in Eastern Europe, and they remain at-large. An area where our Federal Government could help is to force better cooperation from those countries' governments that fail to cooperate in these types of cyber crime investigations and prosecutions.

CYBER SECURITY COLLABORATIVE EFFORTS BY THE FINANCIAL SERVICES INDUSTRY

The FS-ISAC is a member of the Financial Services Sector Coordinating Council (FSSCC) and is viewed as the FSSCC's operations partner. Through the FSSCC, the private sector financial service industry collaborates with Financial and Banking Infrastructure Information Committee (FBIIC) which consists of the key financial services industry regulators involved in critical infrastructure protection such as the U.S. Treasury, the Federal Reserve, the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and others. FSSCC and FBIIC members meet regularly and participate in classified briefings from law enforcement and the intelligence community where important vulnerability and threat information is exchanged.

Financial regulators are actively involved in developing regulations and supervisory guidance and in conducting focused examinations of information security, vendor management and business continuity controls at financial institutions and major service providers. There are nearly a dozen booklets covering these key cyber security and business continuity issues in the FFIEC handbook.

The FS-ISAC also works closely with other key financial services industry groups to protect the industry and its customers against cyber threats. Some of the key organizations have included the ABA, ICBA, FSSCC, NACHA, Regional Payments Associations, BITS and ITAC. The following is a partial list of activities that the financial services sector has undertaken to improve the industry's response to online criminal activities:

- The ABA and ICBA have been instrumental in increasing the membership levels and reach of the FS-ISAC to over 4,200 members today. Through the FS-ISAC's thirty association and processor members, the reach of the FS-ISAC is nearly universal to every regulated financial institution in the U.S., regardless of its size.

- FS-ISAC has worked closely with the Regional Payments Associations to offer regional account takeover workshops for their members. These day-long events consist of presentations from defense in-depth solution providers and include an interactive tabletop exercise that engages the participants in a simulated series of cyber attacks against their financial institutions' customers. Twelve of these workshops have been offered in 2011

and have been supplemented by numerous speaking engagements around the country by the FS-ISAC staff to various conferences.

- The nonprofit ITAC, the Identity Theft Assistance Center, which is part of the Financial Services Roundtable, provides a free recovery service to victims of identity theft. Since its inception, ITAC has helped more than 90,000 consumers recover their financial identities.

ADDITIONAL STEPS THAT INDUSTRY AND THE FEDERAL GOVERNMENT CAN TAKE TOGETHER

Rather than outline a series of recommendations that the financial services industry should take independently and a separate set of recommendations that the Federal Government should address, the following is a consolidated approach for both. This approach better illustrates the need and commitment that we must have for public/private sector cooperation in protecting the industry and the nation's citizens from the growing threat of cyber crime.

1. IMPROVE CYBER CRIME LAW ENFORCEMENT

   a. There needs to be better and more domestic and international collaboration regarding investigations and prosecutions given the origins of a significant portion of cyber crime. Countries that have not adopted the Council of Europe's Convention on Cyber Crime should be encouraged to do so. The Convention is an international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes.

b. Sufficient funding is needed for cyber crime investigations and forensics. Currently, private sector firms report that some local law enforcement agencies require minimum thresholds before they will take the case. However, evidence indicates that most of these types of attacks are directed at many firms and their customers so the cumulative dollar value of the crime committed may be many times the amount of one particular loss.
c. Law enforcement must be more responsive to cyber crimes reported by financial services firms. There needs to be improved communications at a local level between financial services firms and their cyber crime law enforcement contacts and an understanding of how to report these crimes so that action will be taken.

2. IMPROVE FINANCIAL INSTITUTION INFORMATION SECURITY PROGRAMS

Regulators and industry need to have a flexible and dynamic approach to cyber security so that individual financial institutions can continue to improve information security programs based on their size, scope of activities, and structure. This builds on the foundation embodied in the Gramm-Leach-Bliley Act framework and opposes prescriptive, one-size-fits-all or technology-specific approaches.

3. IMPLEMENTATION OF DEFENSE IN-DEPTH SECURITY

Financial services firms and payment processors need to implement defense in-depth security in order to protect their customers and their institutions from cyber criminal attacks. These security solutions must take into account the evolution of the changing threat landscape and will need to be updated over time. Commercially reasonable security procedures must achieve an appropriate balance between security, risk and usability. The June 28, 2011 FFIEC Supplemental Guidance

on Internet Banking Authentication goes a long way towards achieving that balance without dictating any single solution which may prove to be untenable over time.

4. IMPROVE PUBLIC/PRIVATE SECTOR COLLABORATION

Expanded information sharing between government agencies and the financial services industry is one of the FS-ISAC's primary goals. There have been improvements made but there needs to be greater private sector access to threat and intelligence from Federal intelligence and law enforcement agencies. This access must be administered in a manner that can provide broader protection without providing undue market advantage to a select group or that would compromise ongoing investigations. Specific recommendations include:

a. Provide financial institutions, networks and processors with timely, relevant and actionable information on threats, vulnerabilities, and exploits.
b. Provide the financial services industry with analysis of trends using existing data reporting requirements (e.g., FinCEN's data of Suspicious Activity Reports which includes computer crimes).
c. Support the existing National Infrastructure Protection Plan (NIPP) and its supporting organizations such as the National Council of ISACs of which the FS-ISAC belongs and the sector coordinating councils, such as the FSSCC. Also support the FSSCC's public sector partner, the Financial and Banking Information Infrastructure Committee (FBIIC) and support their joint initiatives.
d. Compile and share data on payment system fraud and security trends.
e. Fund top R&D priorities, such as the FSSCC's priority project on identity assurance.

f. Support industry exercises that relate to cyber threats. By routinely engaging in exercises and training, public and private sector participants build relationships and establish trust that is essential for sharing information.

g. Continue towards the goal of a fully integrated Joint Coordination Center for sharing cyber threat information between the public and private sectors. The embedding of financial sector personnel in the NCCIC is a positive step in that engagement process.

5. IMPROVE THE INTERNET INFRASTRUCTURE

Use Federal procurement power to improve the security of software, hardware and services that support the Internet business infrastructure and applications (i.e., enhanced technology that is implementable and cost appropriate for the market.)

6. EDUCATION

More public/private sector collaboration is needed to support educational efforts to increase consumer and business awareness of cyber threats and risk mitigation best practices. One example of such an effort has been undertaken by the National Cyber Security Alliance in promoting a "Stay Safe Online" campaign as part of the October Cyber Security Awareness month (http://www.staysafeonline.org/).

As a result of these types of programs and the efforts of the FS-ISAC Account Takeover Task Force, financial institutions have educated their customers regarding phishing and other social engineering attacks with information on their websites, mailers and in their bank lobbies

regarding safe and secure online banking practices. Corporate and government users of online financial services products can now take advantage of these educational tools that are available.

Thank you again for this opportunity to present this testimony and I look forward to your questions.

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on "Cybersecurity and Data Protection in the Financial Sector"

Before the

Financial Institutions and Consumer Credit Subcommittee

of the

House Committee on Financial Services

September 14, 2011
2129 Rayburn House Office Building,
Washington, DC 20515

Madam Chair and Members of the Subcommittee, thank you for the opportunity to testify today concerning cybersecurity and data protection in the financial sector. My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center ("EPIC"), and I teach privacy law at Georgetown University Law Center.

EPIC is non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues. We work with a distinguished panel of advisors in the fields of law, technology, and public policy. We have a particular interest in promoting technical standards and legal safeguards that help safeguard personal information.[1] I also want to note that U.S. PIRG, a leading consumer advocacy organization, has expressed support for this statement. I would encourage the members of the Committee and their staff to communicate directly with U.S. PIRG as the legislative process moves forward.

We are grateful for the work of this Subcommittee on the critical issues of data security and privacy protection. In my testimony this morning, I will discuss the urgency of this problem, review several recent, high-profile data breaches in the financial sector, and make a few further points about forward-looking strategies for privacy protection. We also want to acknowledge the important enforcement efforts undertaken by federal agencies to protect American consumers, as well as the growing awareness across the financial services sector of the scope of the problem.

There have been several cybersecurity incidents over the past few months that highlight the threats to consumers in the financial services sector. These attacks on financial institutions produce both direct and indirect costs for consumers who must contend with the risk of identity theft and financial fraud, as well as whatever additional costs the companies pass along.

Also, current laws do not adequately protect consumers. In brief, legislation should apply breach notification regulations to financial institutions, should require authentication techniques that reduce the risk to consumers, and should not preempt stronger state laws. Additionally, we favor the development of cyber security policies that are open to public review and comment, that respect the role of the private sector, and that safeguard the rights of consumers and users.

Scope of the Cybersecurity and Data Breach Problem in the Financial Sector

In recent months, there have been many high-profile data breaches in the financial sector. These breaches make clear an ongoing risk to consumers and underscore the need for stronger privacy legislation.

- Just last month, Citigroup suffered two breaches at its Japanese credit card unit, compromising the personal data of over 92,000 consumers.[2] This comes in the wake of one of the most widely reported data breaches of the year, where inadequate security measures at Citigroup exposed customer names, account numbers, and

[1] More information about EPIC is available at the web site http://www.epic.org/.
[2] Dan Goodin, *Citigroup Hit With* Another *Data Leak*, The Register, Aug. 9, 2011, http://www.theregister.co.uk/2011/08/09/citigroup_data_breach_again/.

contact information for more than 360,000 customers in May.[3] Citigroup waited almost a month before it notified its customers.[4] Experts have warned that this disclosure of customer data will make Citigroup customers especially vulnerable to phishing attacks and other acts of fraud.[5]

- In June 15 of this year, Automatic Data Processing Inc. ("ADP"), the largest payroll processor in the world, admitted that the personal data of one of its 550,000 corporate clients was breached, but did not disclose the company that was affected.[6]

- Also in May 2011, news reports revealed that a Bank of America insider had leaked the detailed personal information of many of the bank's customers.[7] As a result of the data breach, the affected customers have lost over $10 million from their accounts.[8] This outcome is particularly troublesome considering that Bank of America is the largest bank in the U.S.[9]

- In January of 2009, weak network security caused a breach at Heartland Payment Systems, a credit card payment processing firm.[10] The company has settled with American Express, Mastercard, Visa, and Discover due to claims raised as a result of the data security breach.[11] It is estimated that millions of consumers' personal card numbers were stolen as a result of the breach.[12] At the time, Heartland claimed to have been compliant with every requirements of the Payment Card Industry Data Security Standard, leading many to cite the breach as an example of the failure of industry self-regulation to protect the private data of consumers.[13]

---

[3] Eric Dash, *Citi Says Many More Customers Had Data Stolen by Hackers*, N.Y. Times (June 16, 2011), http://www.nytimes.com/2011/06/16/technology/16citi.html?_r=1.
[4] Randall Smith, *Citi Defends Delay in Disclosing Hacking*, Wall St. J. (June 13, 2011), http://online.wsj.com/article/SB10001424052702304665904576382391531439656.html.
[5] Jeremy Kirk, *Citigroup Breach Exposed Data on 210,000 Customers*, PC World (June 9, 2011), http://www.pcworld.com/businesscenter/article/229868/citigroup_breach_exposed_data_on_210000_customers.html
.
[6] Maria Aspan, *ADP Says Investigating Data Breach*, Reuters (June 15, 2011), http://www.reuters.com/article/2011/06/15/us-adp-breach-idUSTRE75E5BB20110615.
[7] David Lazarus, *Bank of America Data Leak Destroys Trust*, L.A. Times (May 24, 2011), http://articles.latimes.com/2011/may/24/business/la-fi-lazarus-20110524
[8] *Id.*
[9] National Information Center, *Top 50 Bank Holding Companies in the U.S.*, (March 31, 2011), http://www.ffiec.gov/nicpubweb/nicweb/top50form.aspx
[10] Taylor Buley, *Metadata: World's Biggest Data Breach*, Forbes (January 20, 2009), http://www.forbes.com/2009/01/20/data-breach-metadata-tech-security-cz_tb_0120breach.html
[11] Rachel Chitra, *Update 1- Heartland Payment, Discover Settle Data Breach Claims*, Reuters (September 1, 2010), http://uk.reuters.com/article/2010/09/01/heartlandpayment-idUKSGE6800LT20100901
[12] *Id.*
[13] Jaikumar Vijayan, *Update: Heartland breach shows why compliance is not enough*, ComputerWorld, Jan. 6, 2010, http://www.computerworld.com/s/article/9143158/Update_Heartland_breach_shows_why_compliance_is_not_enough.

- In July of 2008, Wells Fargo, a financial services company and one of the four largest banks in the U.S., was breached by the illegal use of a bank access code.[14] The data breach resulted in the loss of personal information of approximately 5,000 consumers.[15]

- In 2007, TJX, the largest apparel off-price department store in the U.S., announced that it had been the victim of a data breach whereby the personal data of millions of customers was stolen by hackers.[16] The company eventually settled, paying almost $10 million to states,[17] $24 million to Mastercard,[18] and $41 million to Visa.[19]

These problems are not unique to the financial sector. Last month, Purdue University reported that computer criminals had broken into a server containing the personal data of students who attended the university from 2000 through the summer of 2005, and the University of Wisconsin-Milwaukee discovered malware that may have compromised the data of thousands of students and researchers.[20] This summer also saw data breaches at the CIA, the International Monetary Fund, and the computer network of the United States Senate.[21]

Other companies that have recently lost control of sensitive consumer information include: Epsilon, Lockheed Martin, Sony, the Southern California Medical-Legal Consultants, South Carolina's Spartanburg Regional Healthcare System, and the Swedish Medical Center in Seattle. These breaches affected millions of consumers.[22]

---

[14] The Associated Press, *Wells Fargo Data Breach Revealed*, L. A. Times (August 13, 2008), http://articles.latimes.com/2008/aug/13/business/fi-wells13
[15] *Id.*
[16] Aarthi Sivaraman, *TJX Settles Data Breach Case with U.S. States*, Reuters (June 23, 2009), http://www.reuters.com/article/2009/06/23/tjx-idUSN233656120090623
[17] *Id.*
[18] Associated Press, *TJX to Pay Mastercard up to $24M in Data Breach Settlement*, Boston Herald (April 2, 2008), http://www.bostonherald.com/business/general/view.bg?articleid=1084541
[19] Keith Regan, *TJX to Shell Out $41M in Data Breach Settlement*, E-Commerce Times (November 30, 2007), http://www.technewsworld.com/story/60554.html?wlc=1308577476
[20] Journal and Courier, *Purdue warns ex-students of data breach*, Journal and Courier (Aug. 17, 2011), http://www.jconline.com/article/20110817/NEWS0501/108170320/Purdue-warns-ex-students-data-breach; .; Stanley A. Miller II, *UWM computers hacked; data on 75,000 exposed*, Milwaukee Journal Sentinel (Aug. 10, 2011), http://www.jsonline.com/news/milwaukee/127459128.html.
[21] The Economist, An Anonymous Foe, The Economist (June 16, 2011), http://www.economist.com/node/18836210.
[22] Hayley Tsukayama, *Sony, Epsilon Support National Data Breach Bill*, Wash. Post. (June 3, 2011), http://www.washingtonpost.com/blogs/post-tech/post/sony-epsilon-support-national-data-breach-bill/2011/06/02/AG34tvHH_blog.html; Christopher Drew, *Stolen Data is Tracked to Hacking at Lockheed*, N.Y. Times (June 3, 2011), http://www.nytimes.com/2011/06/04/technology/04security.html?_r=3; Press Release, Southern California Medical-Legal Consultants, Possible Data Breach Discovered and Contained (June 11, 2011), http://www.scmlc.com/press.htm; Liana B. Baker & Jim Finkle, *Sony Playstation Suffers Massive Data Breach*, Reuters (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426; SpartanburgRegional, *Letter to Patients*, (May 2011), http://www.spartanburgregional.com/pages/patientnotice.aspx; Carol M. Ostrom, *20,000 Swedish Employees Personal Data Breached*, The Seattle Times (July 20, 2011) http://seattletimes.nwsource.com/html/localnews/2015674739_databreach21m.html.

Many of the data breaches in the non-financial sector still involve the loss of consumers' financial information. For example, gaming companies collect a great deal of financial information. The data breach that affected Sony's PlayStation Network in April exposed the credit card data of 77 million users.[23] The impact of the breach was likely worsened by the fact that Sony waited one week before notifying customers.[24] Examples like Sony's are particularly important because despite the risk to massive amounts of personal and financial data, the privacy risks of online gaming have received little attention from the media or from the federal government.

It is almost impossible to overstate the seriousness of the problem of data breach in the United States. The FBI ranks cyber-attacks as the third greatest threat currently facing the United States, eclipsed only by nuclear warfare and other weapons of mass destruction.[25] According to the Privacy Rights Clearinghouse 500 million sensitive records have been compromised since 2005.[26] The actual number is likely much higher, as many data breaches are never reported in the media.[27] (The Privacy Rights Clearinghouse provides extensive reporting on security breach incidents, including a detailed Chronology that analyzes by year breaches across a wide range of activities and organizations.)[28]

These problems are going to get worse. Indeed, 2011 has already been labeled the "year of the data breach."[29] Financial transactions have already largely moved away from paper, and they are increasingly moving away from the personal hard drive as well. One firm estimates that the global cloud computing market will grow nearly 300 percent by 2014.[30] As more sensitive data moves into the cloud, as we become more dependent on electronic financial records, and as more companies store vast amounts of consumer data on remote servers, the risk that personal data will be improperly disclosed or accessed will necessarily increase.

Moreover, consumers and businesses that become increasingly dependent on these services are less likely to know when problems occur than if they were to lose their own laptop or experience a break-in.

There are several risks to consumers from these data breaches. The most obvious risk is identity theft, which according to the Federal Trade Commission, has been the number one consumer concern for the past decade.[31] EPIC has previously said that the financial services

---

[23] Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive data breach*, Reuters (April 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.
[24] *Id.*
[25] Rick C. Hodgin, *FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs*, TG Daily (Jan. 7, 2009) http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds.
[26] Privacy Rights Clearinghouse, *500 Million Sensitive Records Breached Since 2005*, http://www.privacyrights.org/500-million-records-breached (August 26, 2010).
[27] *Id.*
[28] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, http://www.privacyrights.org/data-breach.
[29] *See, e.g.*, Laura Mather, *The Next New Cyberdefense Strategy: Monitor Everything*, TechNewsWorld (Aug. 27, 2011) http://www.technewsworld.com/story/73162.html?wlc=1315672890
[30] *See* Eugene A. Ludwig, *Data Insecurity is a Systemic Threat*, BankThink (Aug. 16, 2011) http://www.americanbanker.com/bankthink/breach-hack-data-security-systemic-risk-1041244-1.html.
[31] Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2010,

industry bears some blame for identity theft concerns because the credit granting system and electronic payment mechanisms are designed in a way that makes committing fraud easy.[32] The industry favors convenience over security because tolerating some identity theft is often more profitable for companies.[33]

We have also cautioned against the financial services industry's solution of requiring more personal information, including biometric systems, to authorize charges. These systems raise serious privacy and security risks.[34] Instead, we suggest that the best way to minimize the problem of identity theft is to reduce the industry's use of the social security number as a personal identifier.[35]

Unfortunately, identity theft is only one risk from unauthorized access to personal information.[36] Unauthorized access may be gained for other purposes that cause harm to the individual, such as stalking, corporate espionage, extortion, or to supply information that will be used in future phishing or fraud activities.

The recent breach at Citigroup is a good example of this. The information originally obtained in the breach may not have included social security numbers, credit card numbers, or other traditional tools of identity theft, but it was enough to leave consumers vulnerable to phishing attacks. Spear phishing is a more effective and targeted version of phishing as the source of the e-mails sent to the potential victims comes from a supposedly trusted or known source.[37] In instances such as this, consumers should be notified so that they can take proper precautions against future attacks and possible fallout from the data breach.

New Threats to Web Site Security Certificates

In addition to data breaches in the financial sector, consumers are facing a new threat to their private information from security breaches at companies that issue digital security certificates.[38] In August 2011, the web security firm DigiNotar, a holder of digital security certificates, revealed that it had been breached by a computer criminal who stole authentication certificates used by dozens of popular companies, including Google, Microsoft, Facebook, Twitter, and Yahoo, as well as government entities like Israel's Mossad, Britain's MI6, the CIA,

---

http://www.ftc.gov/opa/2011/03/topcomplaints.shtm; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2009, http://www.ftc.gov/opa/2010/02/2009fraud.shtm; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2008, http://www.ftc.gov/opa/2009/02/2008cmpts.shtm; Federal Trade Commission, FTC Releases List of Top Consumer Complaints in 2007, http://www.ftc.gov/opa/2008/02/fraud.shtm.

[32] EPIC, Identity Theft, http://epic.org/privacy/idtheft/ (last visited June 17, 2011).

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] EPIC, *Testimony for the Legislative Hearing on "Data Security: The Discussion Draft of Data Protection Legislation"*(July 29, 2005), http://epic.org/privacy/choicepoint/datasec7.28.05.html.

[37] Ross Kerber and Diane Bartz, *Analysis: Data Breach Shows New "Spear-Phishing" Risk*, Reuters (April 5, 2011), http://www.reuters.com/article/2011/04/05/us-hackers-epsilon-idUSTRE7336DZ20110405

[38] The Associated Press, *Hacking in the Netherlands Took Aim at Internet Giants*, New York Times (Sept. 5, 2011), http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html?hpw.

and most of the Web sites of the Dutch government.[39] In total, fraudulent certificates for 531 domains were generated.[40]

Digital security certificates are used to authenticate Web sites and to ensure the security of communications between a Web site and a user's browser. With fraudulent security certificates, a computer criminal could direct users to fake websites and trick them into revealing their usernames, passwords, and other private information. For example, the holder of a fraudulent Google certificate could set up a website under a legitimate Google domain name. Consumers who visited such a site would put their personal information at risk. Technology experts believe the attack is connected to Iran, citing the presence of nationalist slogans in Farsi and the fact that only a government with control over an Internet service provider could direct Internet traffic to the spoofed Web sites.

The computer criminal allegedly responsible for the attacks calls himself the "Comodohacker," a reference to a breach at Comodo, another holder of digital certificates, for which he claimed credit. Though he claims to be an independent, Iranian software engineering student, Comodohacker admits to sharing the information he uncovers with Iran.[41]

In the years ahead, the threat posed to consumers by fraudulent security certificates will increase. Indeed, only a few days ago the digital certificate firm GlobalSign had its Web site breached by a computer criminal.[42] As a result of these threats, consumers are exposed to a "new and extremely dangerous cyber crime threat"[43] when they interact with companies, like those in the financial sector, that are involved in the collection of sensitive information.

General Recommendations

In our view, none of the current legal frameworks provide adequate safeguards for consumers, bank customers, depositors, and others who provide personal information to obtain financial services.

In general, EPIC supports cyber security laws that feature an opt-in approach for companies' use of personal information, that allow for private rights of action for consumers, and that do not pre-empt state data breach legislation. To address similar data breach problems in the communications sector, EPIC has recommend several security measures that telecommunications firms could use to protect the privacy of customer data.[44] These measures include: authentication

---

[39] *Id.*
[40] Gregg Keizer, *Hackers steal SSL certificates for CIA, MI6, Mossad*, ComputerWorld (Sept. 4, 2011), http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad.
[41] Somini Sengupta, *Hacker Rattles Security Circles*, NY Times (Sept. 11, 2011), http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html.
[42] *Id.*
[43] Matt Liebowitz, Cracked digital certificates endanger 'web of trust', MSNBC.com (Sept. 7, 2011) http://www.msnbc.msn.com/id/44430823/ns/technology_and_science-security/t/cracked-digital-certificates-endanger-web-trust/#.Tm5gmo6omVo.
[44] EPIC, *Petition to the Federal Communications Commission for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information* (Aug. 30, 2005) at 15, *available at* http://epic.org/privacy/iei/cpnipet.html.

by consumer-set passwords instead of biographic identifiers like date of birth or social security number; audit trails that record all instances where a customer's record is accessed; encryption of stored data; notice to the affected individuals and the relevant agency when there is a security breach; and limiting data retention by either deleting call records after they are no longer needed or divorcing identification data from the transactional data.[45] Similar security measures should be applied in the financial sector.

Data breach notification laws can also help us understand the extent of the data breach problem so that better safeguards and practices can be developed. EPIC supports notification laws that contain data minimization, that require short time periods for notification, that contain a sufficiently broad definition of "Personally Information," and that take advantage of social networks and text messaging for notification.

Finally, we favor the development of cyber security policies that are open to public review and comment, that respect the role of the private sector, and that safeguard the rights of consumers and users.

I will briefly outline each of these recommendations below.

Opt-In Standard

EPIC has previously suggested that laws such as the Gramm-Leach-Bliley Act ("GLBA") can be improved by giving consumers the option to opt-out of some sharing of personal financial information.[46] Currently, GLBA gives consumers the right to opt-out from a limited amount of nonpublic personal information sharing. Specifically, a consumer can direct the financial institution to not share information with unaffiliated companies.

These types of opt-out approaches unfairly place the burden on the individual to protect privacy and thus weaken customer power to control their financial information. Most privacy and opt-out policies are usually convoluted, confusing, and misleading since they are created by entities whose interests are better served when there is no effective notice. Instead, financial institutions should implement an opt-in approach to the use of personal information because this minimizes any unwanted or unknowing disclosure of information and places the burden of responsibility on those actors who will gain from the disclosure of information.

Private Right of Action

EPIC supports data protection laws that contain a private right of action for consumers.[47] Private rights of action strengthen enforcement and allow individuals to seek remedies.

---

[45] *Id.*

[46] *Hearing on "Cybersecurity and Data Protection in the Financial Sector,"* (June 21, 2011) (Testimony of Marc Rotenberg, EPIC, to Senate Committee on Banking, Housing, and Urban Affairs), *available at* http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf; *see also* EPIC, The Gramm-Leach-Bliley Act, http://epic.org/privacy/glba/ (last visited September 11, 2011)..

[47] *See Hearing on "Cybersecurity and Data Protection in the Financial Sector,"* (June 21, 2011) (Testimony of Marc Rotenberg, EPIC, to Senate Committee on Banking, Housing, and Urban Affairs), *available at*

Additionally, because it is often difficult to place a dollar value on data breaches and privacy infringements, it is important that any private right of action also include a statutory damages provision. This would empower consumers to enforce the law themselves and create a strong disincentive for the irresponsible handling of consumer data. Not only would this provide the opportunity for individuals who have been harmed by security breaches to have their day in court, it would also provide a necessary backstop to the current enforcement scheme, which relies almost entirely on the Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights.

For these reasons, many state laws include private rights of action. California, Hawaii, Louisiana, and Washington, for instance, include provisions in their state data breach laws that allow consumers to bring a civil action and recover damages.[48]

Data Breach Notification

EPIC supports notification bills that contain data minimization provisions.[49] It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks occur is to collect less sensitive personal information at the outset. It is the credit card numbers, the bank account numbers, the social security numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces this vulnerability. The simple message to business should be "if you can't protect it, don't collect it."

Data minimization provisions like those found in the Secure and Fortify Electronic Data Act ("SAFE Data Act") are a good start, but we would urge you to go further. Instead of simply a data minimization plan, we would recommend a data minimization requirement. There are many examples of this already in privacy law. For example, the Video Privacy Protection Act requires businesses to:

> Destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information . . . .[50]

Second, EPIC supports short time period requirements for notification. EPIC previously testified before the House Commerce Committee in support of the SAFE Data Act's 48-hour requirement for breach notification.[51] Short time periods require companies to respond quickly

---

http://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

[48] Cal. Civ, Code § 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 et seq. (2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).

[49] *See Legislative Hearing on "Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach"* (June 15, 2011) (Testimony of Marc Rotenberg, EPIC, to House Committee on Energy and Commerce and Subcommittee on Commerce, Manufacturing, and Trade), *available at* http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

[50] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (Nov. 5, 1988), *codified at* 18 U.S.C. 2710.

[51] *See Legislative Hearing on "Discussion Draft of H.R.____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach"* (June 15, 2011) (Testimony of Marc

when there is a problem and allow consumers to react more quickly and take preventative or mitigating actions.

Notification laws should also contain a sufficiently broad definition of "Personal Information." This definition is critical because, as with most privacy bills, this definition will determine when the obligations of a notification law should be applied and when they can be basically ignored. EPIC has previously suggested that bills such as the SAFE Data Act should define Personal Information as information that "identifies or could identify a particular person," followed by the examples cited in the Act as illustrations, with those illustrations qualified by the phrase "including, but not limited to."[52] This approach is technology neutral, less dependent on the rulemaking process, and more likely to adapt over time.

Additionally, the definition of Personal Information should *not* exempt "public record information" available from federal, state, or local government systems that was acquired by the company that suffered the breach for public purposes. If an organization suffers a security breach of confidential information or of "public information," it has a problem that needs to be corrected. If no action is taken to correct the problem, it is quite likely the breach will occur again. Thus, even when there is no immediate harm to the individual, the problem remains and the security obligation should apply. Also, I would not assume that a data breach of public information merely discloses the equivalent of what could be found through public data sources. It is quite likely, particularly in the information broker industry, that the "public" information contained in a particular data record is far more detailed than any record that would be available in a single government record system.

Finally, breach notification laws should take advantage of text messaging and social networks as methods of notification. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But it is an effective way of quickly notifying consumers of the problem and of making them aware that they should look for a notice that might arrive in the mail or show up in the email box.

In a similar spirit, where a bill speaks of providing notification by means of a web site, it may be appropriate to add "or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

Preemption

Many Senate and House data breach bills, such as the SAFE Data Act, preempt state laws that have similar security obligations as well as state laws that provide for data breach

---

Rotenberg, EPIC, to House Committee on Energy and Commerce and Subcommittee on Commerce, Manufacturing, and Trade), *available at* http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

[52] *Id.*

notification. If enacted, the federal laws would preempt more effective state information security legislation and foreclose future legislative innovation at the state level.

EPIC's view is that it would be a mistake to adopt preemption provisions of this type. Businesses understandably will prefer a single national standard. That is the argument for preemption. However privacy laws have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish. This approach to consumer protection is based upon our federalism form of government that allows the states to experiment with new legislative approaches to emerging issues. It is important that states be permitted to legislate in this area. As discussed already, most states have comprehensive data breach legislation. Often, this legislation establishes a private right of action, statutory damage scheme, and notification requirements. [53]

Because states enjoy a unique perspective that allows them to craft innovative programs to protect consumers, they should be permitted to continue to operate as "laboratories of democracy" in the privacy and data security arena. State legislatures are closer to their constituents and the entities they regulate; they are the first to see trends and problems, and are well-suited to address new challenges and opportunities that arise from evolving technologies and business practices. This is why privacy bills have typically created a federal baseline and allowed the states to adopt more stringent safeguards if they wish.

There is an additional reason that we believe weighs against preemption in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge. California, for example, has recently updated its data breach notification law to specify the information that should be provided by data holders to individuals in the event of a breach and to require that the state Attorney General be notified in the event of a large breach.[54] Massachusetts is also considered updates to its data breach law in response to new threats.[55] It is very likely that the states will continue to face new challenges in this field. Placing all of the authority to respond here in Washington in one agency would be, as some in the security field are likely to say, a "critical failure point." The temptation to establish a national standard for breach notification should be resisted, particularly given the rapidly changing nature of the problem.

White House Draft Cybersecurity Legislation

The White House has recently unveiled a Cybersecurity Legislative Proposal that seeks to "improve critical infrastructure protection by bolstering public-private partnerships with

---

[53] *See e.g.* Cal. Civ. Code 1798.82 (2011).
[54] *See* EPIC, California Passes Updated Data Breach Legislation, http://epic.org/2011/09/california-passes-updated-data.html (last visited September 11, 2011).
[55] Jason Gavejian, *California and Massachusetts Legislatures Push Data Breach and Security Bills,* Workplace Privacy, Data Management, and Security Report (May 3, 2011), http://www.workplaceprivacyreport.com/2011/05/articles/workplace-privacy/california-and-massachusetts-legislatures-push-data-breach-and-security-bills/.

improved authority for the Federal government to provide voluntary assistance to companies and increase information sharing."[56]

The Proposal would grant DHS the authority to develop and conduct risk assessments of Critical Information Infrastructure (CII) and foster the development...of essential information security technologies and capabilities for protecting federal systems and [CII].[57] CII is defined as "any physical or virtual information system that controls, processes, transmits, receives, or stores electronic information in any form...that is vital to the functioning of critical infrastructure, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, *national economic security*, or national public health or safety, or owned or operated by or on behalf of a state, local, tribal, or territorial government entity."[58] This would seem to include the financial services industry in its broad sweep.

EPIC welcomes the White House's efforts to strengthen our nation's cybersecurity and privacy protections for financial information. While the White House states that "[p]rotecting civil liberties and privacy rights remain fundamental objectives in the implementation of the [Cybersecurity Legislation],"[59] we would warn the Subcommittee about the provisions giving control over "critical information infrastructure" (CII) to the DHS. The definition of CII is quite broad and it is important to ensure that any cybersecurity proposal does not lead to increased government monitoring of private information.

Furthermore, it is important to reiterate that cyber security policies should allow for public review and comment, respect the role of the of the private sector, and safeguard the rights of consumers and users. I make this point because there is the very real risk that in the realm of cyber security much of the authority for legal compliance and technical standard-setting could be too easily turned over the National Security Agency. Already the NSA has suggested that the government may need to monitor private networks and assist in the development of key technical standards.

This would be a grave mistake. In fact, if the NSA had had its way twenty years ago in the battle over cryptography standards for the Internet, it is quite likely that the vulnerability of US networks to attack would be much greater than it is today. This should be of particular concern to those watching closely the recent cyber security developments in the financial services sector.

Department of the Treasury's Financial Crimes Enforcement Network Reporting Proposal

---

[56] *See* White House: Legislative Language, Law Enforcement Provisions Related to Computer Security (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf. [hereinafter "White House Legislative Proposal"].
[57] White House Legislative Proposal, *supra* note 39 at 22.
[58] *Id.* at 20. Emphasis added.
[59] The White House, *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited June 20, 2011).

The Treasury Department's Financial Crimes Enforcement Network recently proposed new regulations that would require banks to report all international electronic money transfers.[60] The regulation would significantly expand the transfer of bank record information to the US Treasury Department and law enforcement agencies. Where such data collection is necessary, EPIC favors a narrowly focused approach in which the government knows beforehand which data is associated with terrorist financing, and pursues only that data.

Conclusion

Financial privacy protections need to be strengthened in the U.S. The rise in significant data breaches and the problem of I.D. theft indicate clearly that more must be done in this area to protect financial data. Moreover, the emergence of attacks on issuers of digital certificates, raises new concerns about online security.

We support legislation that strengthens safeguards for consumer information and promotes data minimization practices. Specifically, we urge the adoption of techniques that minimize the collection of personally identifiable information. These techniques reduce the risk of cyber attack and minimize the risk to consumers when attacks occur.

We also support strong notification requirements so that consumers are not left out of the loop when breaches occur. Private rights of action and statutory damages provisions are also important to empower consumers and increase enforcement. Companies also need to know that they will be expected to protect the data they collect and that, when they fail to do so, there will be consequences. Legislation for information security and breach notification is needed, but it should not preempt stronger state measures and it should not rely solely on FTC rulemaking authority.

We broadly favor Administration efforts to promote cybersecurity. But we caution against Government overreaching that leads to increased monitoring of private communications or technical standard-setting that makes communications and databases more vulnerable to attack.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

---

[60] *See* EPIC, *US Government Seeks to Monitor All Money Transfers,* http://epic.org/2010/09/us-government-seeks-to-monitor.html (last visited September 11, 2011).

TESTIMONY OF
A. BRYAN SARTIN
VERIZON COMMUNICATIONS

BEFORE THE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS & CONSUMER CREDIT
COMMITTEE ON FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

ON
"CYBER SECURITY: THREATS TO THE FINANCIAL SECTOR"

SEPTEMBER 14, 2011

Chairman Bachus, Ranking Member Frank and members of the Subcommittee, thank you for the opportunity to testify today on cyber threats to the financial services sector. My name is Bryan Sartin and I am the director of Investigative Response for Verizon. I have been closely involved in the information security space for more than 15 years, with a particular focus on assisting both commercial and government entities in responding to cyber-related attacks.

The Verizon Investigative Response (VZIR) group handles all digital forensics, computer incident response, electronic discovery and information technology (IT) investigations requested by Verizon customers. It is a specialized team of IT investigators, hailing from four primary backgrounds: law enforcement, military, systems engineering and institutional IT. We maintain a full-time presence in 14 countries and handle more than 200 cases each year, including a significant percentage of the investigations behind many of the world's most publicly visible data breaches.

Much of the key risk and threat related findings stemming from VZIR casework is documented in an annual publication known as the Verizon Data Breach Investigations Report (DBIR). This year's study, released in March, was published jointly by Verizon, the United States Secret Service, and the Dutch National High Tech Crime Unit. This study encompasses more than 1,700 data breaches, over seven years of research, and more than 900 million stolen records. This is a study of security failures and the lessons that can be learned from them.

Based on my industry experience, my duties as head of the VZIR team, and as a co-author of the DBIR, I want to offer the following points for the Subcommittee's consideration:

- Although the consequences of cyber attacks may differ depending on the target, there is little variance in cyber risks and threats by sector.
- While cyber threats continue to evolve rapidly and can be executed at the speed of light, in reality most cyber crimes are typically not complex, sophisticated or fast moving.
- While there is no panacea for the prevention of a breach, the most fundamental security controls make the most effective countermeasures.
- Many businesses and other entities that are data breach victims fail to rapidly recognize and react to the lead indicators of the cyber attacks committed against them.
- Affording cyber victims some protection from litigation, fines and penalties will encourage cooperation with law enforcement, will promote successful criminal prosecutions, and will likely reduce the overall numbers of electronic crimes.

Before exploring each of these points in greater detail, I would like to provide the Subcommittee with some background information that illustrates where the VZIR team fits in the overall Verizon network security program.

Securing the Verizon Network and Keeping Customers Safe

As a provider of communications services, Verizon manages thousands of voice, video, and data networks at the local, regional, national, and international level. Our data network spans six continents and reaches customers in more than 2,700 cities and 150 countries. We serve tens of thousands of businesses and government agencies, including 97% of Fortune 500 companies and roughly 10 million residential broadband customers here in the United States.

As a large corporate enterprise and provider of communications services, Verizon engages in a wide range of activities to enhance cyber security for ourselves, our customers, and other users of our network. These activities take place at many different layers within our organization. For example, we work closely with our vendors so that that their products are able to meet our security architectures and requirements. In addition, Verizon's network security group invests in a variety of tools, security sensors, and other technologies to identify and mitigate threats in cyberspace as they are emerging. Every day, we find and remove spam, phishing, denial-of-

service and other malicious activity that threaten to disrupt our network or our customers' use of it. We help customers secure their networks and data by offering managed firewall, intrusion detection and prevention, and encrypted virtual private networking services. We also offer security consulting, network analysis, incident response, and computer forensics.

It is this latter function — customer-facing security consulting, network analysis, incident response, and computer forensics — that is handled by the VZIR team, and the 2011 DBIR that I co-authored is an example of our activities in this area. This report uses an information-sharing framework called Verizon Enterprise Risk Incident Sharing (VERIS), which Verizon developed and has published as an open-source initiative. The DBIR report also provides valuable advice and guidance for corporate and government entities on tangible, effective steps they can take to better secure their networks today. Financial services firms are among the beneficiaries of the information we make available.

I would like to now offer more detailed information regarding the five points I identified earlier.

Little Variance in Electronic Crimes Risks and Threats by Sector

The 2011 DBIR shows that Hospitality (40%), Retail (25%), and Financial Services (22%) represent the top three sectors in terms of data breach victims. Cyber criminals are after data they can easily convert into cash. More than 90% of all electronic crimes included in the 2011 DBIR are financially motivated in nature.

Retailers and financial services entities tend to have the largest quantities of the data types most frequently targeted. Our research shows that the kinds of data that cyber criminals most frequently target are payment card records, such as credit card, debit card and PIN information. That was true in 78% of more than 1,700 cases. Authentication credentials, such as usernames and password combinations, are the second most frequently targeted at 45%. Other types of personally identifiable information or PII are third at 15%[1].

For this reason, these entities have been and will likely continue to be key targets of electronic crimes, as will small- to mid-size businesses that handle similar data types but in lower quantities and have less developed information security countermeasures.

It is not entirely true, though, that these sectors face a unique cyber security threat landscape as compared to other sectors or industries. There is a misperception that cyber security risks and threats are sector-specific and unique. Financial IT security experts, for example, are often

[1] Note that any single data breach may show many different types of stolen records.

quick to dismiss intelligence drawn from other sectors under the presumption that no applicable lessons can be learned. That's a critical mistake. Similarly, American companies can learn much from intelligence drawn from data breaches affecting foreign entities. Our research and experience shows that cyber risks and threats are not unique to sectors or even geographies.

To the extent that subtle differences exist, these tend to manifest in organized crime rings that prefer specific language sets (e.g., Japanese versus English) or have insider knowledge of certain companies or industries. Cyber threats vary by the kinds of data that a given entity stores, handles or transmits, as opposed to varying by industry, sector or geography. Thus, cyber crimes taking place in foreign jurisdictions, as well as those targeting victims in other sectors, present applicable and compelling IT intelligence. This point particularly applies to governments, financial services, retail and hospitality companies. Hard lessons cannot be dismissed on the grounds those lessons were learned by someone else.

Cyber Crimes Do Not Require Great Complexity or Sophistication to Succeed

Electronic crimes generally do not involve complexity or innovation on the part of the perpetrators. The 2011 DBIR shows that nine of the top ten hacking methods employed in electronic crimes over the past seven years are very simple in nature. Best-in-class information security often reflects a "defense in depth" practice and avoids reliance on just one mechanism – such as a password – to secure functions or assets. Consider the following:

- Exploitation of default or easily guessable credentials accounts for 67% of cases and 30% of stolen records. Many devices often ship with default user names and passwords—such as "admin" and "password1." If not changed, use of these pre-existing default credentials offers cyber thieves an easy entry point.

- Brute force and dictionary attacks account for 52% of cases and 34% of records. We are all familiar with systems that lock-out users after some number of failed login attempts, but failure to implement such mechanisms can enable criminals to use automated tools to try vast combinations of usernames and passwords in rapid-fire succession, often leading to successful access to the system.

- Usage of stolen login credentials accounts for 21% of cases and 21% of records. For example, a criminal could purchase user account names and passwords and utilize that information to obtain unauthorized access to a victim entity from across the Internet.

- Exploitation of insufficient authentication accounts for 10% of cases and 21% of records. An example of this could involve a criminal attempting to obtain unauthorized access across the Internet to an application run by a victim entity and then finding that no login is required.

Unlike cyber threats on the Internet, where fast-moving worms or viruses can quickly propagate across vulnerable systems in a matter of seconds or minutes, actual criminal activities targeted at infiltrating and extracting data from end-user organizations do not appear to be becoming more complex or sophisticated, faster moving or more pervasive, at least not based on the data breaches that we've investigated. If anything, the techniques being used to infiltrate and exploit identified end-user data systems are evolving toward the less complex and commoditized.

In 2010, VZIR group, the United States Secret Service and the Dutch National High Tech Crime Unit investigated more unique data breach events than in any prior year. Remarkably, only five patchable vulnerabilities were found exploited.

An application or computer system vulnerability is considered "patchable" when it is known to be problematic and its discovery is followed by the release of a fix or patch addressing that vulnerability. This suggests that criminals do not need to exploit application and computer system vulnerabilities when easier pathways of unauthorized access exist, such as those listed above. Stated another way, our research shows that with so many weak and easily exploited targets of opportunity available, great complexity and sophistication are not necessary for cyber crimes to succeed.

Fundamental Security Controls are the Most Effective Countermeasures

Our research suggests that most electronic crimes could be more easily prevented than most anticipate. If the tools and tactics employed by criminals are increasingly basic, even commoditized, then indeed the most effective countermeasures are similarly simple. The 2011 DBIR shows that 71% of initial points of entry in international electronic crimes traverse remote access facilities in use by the victim entity. Remote access refers to virtual private networks (VPN), remote control and remote node applications in particular. These are remote access facilities made available to mobile employees and external IT support vendors. Of these, local remote screen sharing applications such as remote desktop and *PCAnywhere* account for 64% of avenues of intrusion. Online session screen sharing, such as *LogMeIn*, *Go2Assist*, and *NetViewer* account for 5%. Remote shell applications such as *SSH* and *Telnet* and Web-based terminal applications such as *Citrix* and *Microsoft Terminal Services* account for 2% each.

Our research does not indicate that there are systemic security flaws in these applications. Instead, the underlying problems stem from the manner in which these applications are deployed and configured by the victimized entity. Most remote access points of entry found in electronic crimes investigations tracked by the DBIR could have been prevented if the targeted remote access facility or application required a second factor for authentication. For example, if these remote access facilities required end users to authenticate with user name and password, as well as a hardware or software token, most unauthorized access could have been prevented. This is compelling intelligence.

Another addressable vulnerability exists because of a lack of controls found on outbound traffic. The 2011 DBIR shows that 92% of data breaches are external to the victim entity. In other words, criminals access a victim's facilities through wireless networking or some other external avenue of intrusion. Once they've gotten into the victim's system, cyber criminals must then find data of interest or value for the purposes of exfiltration. They must gain unauthorized access, find data and get it out without being noticed.

Most victims of external data breaches, both public and private sector, focus security countermeasures almost entirely on defending the network perimeter against unauthorized access. This is only a start. Making it difficult or impractical for criminals to exfiltrate stolen information is an equally effective way to prevent data breaches. Unfortunately, this approach is underutilized.

Significant Improvement in Breach Detection is Needed

2011 DBIR findings indicate that there is often a significant time lag between when a breach occurs, when data theft actually occurs and when the victim discovers the breach. This ranks among the most surprising intelligence offered by the studies, according to reader feedback. Consider the following points:

- Over the past seven years, the timeframe from initial point of entry to the first verifiable instance of data theft is more often measured in days (44%), weeks (5%) or months (4%), as opposed to minutes (33%) or hours (14%).

- The timeframe from initial point of entry to the point the victim entity first discovers the possibility of a data breach is, on average, just over 6 months.

- Even after 6 months, 86% of victim entities did not find evidence of data breach on their own – 46% found out about the problem via 3rd party fraud detection, 30% were notified by law enforcement and 6% were reported by customers or business partners who were also affected.

The very same part of the 2011 DBIR shows that in terms of data breach detection methods, countermeasures such as anti-virus, intrusion detection systems including intrusion prevention, and log review processes account for only negligible percentages (<1%). No one should infer, however, that these countermeasures are not effective.

On the contrary, our research suggests that security controls such as intrusion detection systems and log review processes are effective countermeasures when deployed as part of a defense-in-depth approach. However, at times, our VZIR team found deficiencies in the manner in which these systems were deployed and configured. Worse, even greater deficiencies were found in how these systems were operated by the victim entity on a day-to-day basis.

Deficiencies in logging and, of equal importance, meaningful reviews of logging, are factors contributing to the success of a cyber attack. Often, logging facilities are available but are disabled or reduced in capacity for performance or cost reasons. Failure to utilize log data showing inappropriate activity through a mechanical or manual review provides "cover" for bad acts. Notwithstanding the fact that some details of almost every data breach can be found in logs, victim entities rarely discover the problem on their own even after six months. As a result, real world data breaches play out over considerably longer timeframes than most anticipate.

Closer Law Enforcement Cooperation Could Reduce Overall Numbers of Electronic Crimes

Greater sharing of electronic crimes intelligence between private industry victims and law enforcement has enabled a dramatic improvement in investigative techniques and the ability of investigators to identify perpetrators conclusively. Such identification is critical to successful prosecution which, in turn, has a discernable impact in reducing cyber crimes thereafter.

The 2011 DBIR details the extent to which data breaches (92% of the total case population) can be conclusively tied back to known organized crime groups (58%), unaffiliated persons (40%), and other known adversaries. More often than not, such a conclusive identification of perpetrator(s) is possible. It shows that as of December 31, 2010, only 14% of data breaches revealed unknown or otherwise unidentifiable sources. This is significant; just a few years ago, that number was closer to 65% (based on Verizon-only figures).

With each month that passes, investigators become more capable of identifying data breach perpetrators. The discovery of common artifacts across distinct case investigations, including but not limited to IP address sources, malcode samples, attack sequences and underground chatter, makes it possible to not only reveal perpetrator(s) but also better set the stage for successful arrest and prosecution.

Open source efforts such as the VERIS framework allow for the sharing of cybercrimes intelligence among investigative groups having disparate jurisdictions and focus. In fact, the VERIS framework served as the information-sharing vehicle making the DBIR possible.

The greatest obstacle to cooperative information-sharing is the reluctance of cyber victims to engage law enforcement. VZIR often encounters a misperception by victim entities, however inaccurate and unfounded, that notification of law enforcement is tantamount to an open public disclosure. They avoid such notification in an attempt to sidestep fines, penalties and general dispute litigation stemming from disclosures. Further, when law enforcement authorities are already involved, this perception drives data breach victims to cooperate only in part or to the minimum extent necessary.

While notifications to consumers serve an important role to protect individuals in certain instances, a notice is most effective when it is limited to instances where the breached data elements impose an actual risk of harm, such as a social security number or financial account number. Requiring consumer notifications for data elements that do not create a risk of harm or for identifiers that do not personally identify individuals are an unnecessary exercise that does not serve any of the stakeholders. Consumers may find such notifications confusing and learn to ignore them, eventually ignoring those that they should truly pay attention to.

Reasonable protections for victims of cyber crimes from litigation and regulatory fines would encourage cooperation between those victims and law enforcement. It would improve the odds of successful criminal prosecutions. Our research supports the notion that visible prosecution tends to have a measurable impact on total numbers of electronic crimes immediately thereafter.

Perhaps the most significant development over the past several years was the unexpected drop in IT investigations demand internationally following the Al Gonzalez arrest and prosecution here in the U.S. in 2009. During the following five-month period, VZIR observed a considerable ease in customer-demand. This finding was echoed by industry partners and in public sources of data breach disclosure tabulations. Promoting full cooperation with law enforcement and improving information sharing pathways are among the most positive steps that can be taken today to diminish the electronic crimes risks and threats we collectively face.

Government's Role in Promoting Cyber Security

As the prior discussion illustrates, there is a role for government to play in helping end users better defend themselves against advancing cyber crimes. First, government can leverage its capabilities to help conduct research and development into cyber security best practices for

end user entities. Sponsorship of fundamental educational initiatives in the area of cyber and computer security -- whether it be curriculum development for K-12 students, or advanced contests for graduate students and private sector -- can all help lead to a better equipped cyber security workforce.

Similarly, the government could take to heart many of the recommendations in the DBIR and other industry studies, and use those as a model for securing its own networks and infrastructure. Using government procurement power to dictate security requirements for systems and applications deployed by the government can go a long way to funding the availability of such resources for the private sector.

In that same vein, a single, national paradigm for reporting of high risk security breach incidents to affected individuals is crucial. With over forty different state requirements on when and how to give notice, an organization's compliance resources are wasted instead of being put to use for improving cyber security. In today's increasingly mobile society, consumers should be able to rely on a uniform and risk based process to notify them of breaches that impose a true impact on their privacy and identity. As noted above, it does not help consumers to be overwhelmed with notices of every incident, but rather meaningful notices of incidents which represent a reasonable risk of identity theft in a manner that is recognizable and efficient.

It is important to realize that there is no guarantee that an entity can make against every breach. As we have discussed above, there are some reasonable measures entities can take. An important role for government is to implement laws and incentives that enable an entity to take advantage of a safe harbor when it has proactively subscribed to a set of practices or a self regulatory program. The ultimate goal for consumers and all stakeholders should be greater information sharing and cooperation with law enforcement.

It has also been suggested in several legislative proposals that the government work with small- and medium-sized businesses to facilitate technology-transfers in the area of computer and information security.

Finally, the government should implement processes to share threat and vulnerability information with end users. In its law enforcement role, government is likely to come into possession of a vast trove of data about perpetrators, exploits, means, methods—and most notably, other potential victims. Figuring out ways to quickly disseminate information to other potential (or actual) victims presents possibly one of the biggest opportunities for beneficial government involvement in securing our nation's network-dependent industry sectors.

Conclusion and Recommendations

Cyber attacks represent very real threats to our economic prosperity and our national security. While many public and private sector remediation activities have been highly advanced and effective, our data breach investigations indicate that even greater vigilance is required. The 2011 DBIR lays out several recommendations which, if implemented, would improve the cyber security posture of financial services firms specifically and of the private and public sectors more generally. Overall, it's critical for every entity to identify a set of essential controls and to ensure their implementation across the organization without exception. More advanced controls can be implemented as necessary. The overarching message behind those recommendations is to achieve *essential* first and then worry about *excellent* later.

Remediation activities can be even more effective if legislation clearly articulates public and private sector roles and responsibilities. Government's role in helping to secure cyberspace centers on setting the example by operating highly secure networks, building strong partnerships with the private sector and improving online users' cyber-preparedness.

Mr. Chairman, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing end user information systems and networks. I look forward to answering any questions you may have.

Statement for the Record
of
Greg Schaffer
Acting Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Financial Services,
Subcommittee on Financial Institutions and Consumer Credit
Washington, DC

September 14, 2011

Introduction
Chairwoman Capito, Vice Chairman Renacci, Ranking Member Maloney, and distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission with a particular focus on efforts to reduce cybersecurity risks posed to the Banking and Finance Sector.

Cybersecurity threats to critical infrastructure and services endanger their confidentiality, integrity and availability. DHS, working with our federal partners, assists the private sector in countering these threats and mitigating vulnerabilities in critical systems. This mission is especially critical to the financial sector in today's climate of growing economic and national security concerns. The Department is committed to working more closely with this subcommittee to reduce risk across the Banking and Finance Sector while increasing our cybersecurity posture. To achieve our shared goals, we need to increase the sharing of timely and relevant intelligence information concerning cybersecurity threats with financial sector stakeholders while increasing public awareness of the important role cybersecurity plays in ensuring safe and reliable banking and financial services.

The Current Cybersecurity Environment in the Banking and Finance Sector
The Banking and Finance Sector provides critical deposit, consumer credit, and payment processing services that have become integral aspects of everyday life. As with other U.S. critical infrastructure sectors, financial institutions face a combination of known and unknown vulnerabilities, including the expansion of adversaries' capabilities and challenges to threat and vulnerability awareness. Because financial institutions are critical to the Nation's economic security and handle large sums of money, malicious actors find them to be especially attractive targets. There are also risk considerations associated with the Banking and Finance Sector's dependencies on other critical infrastructure sectors. In simple terms, financial transactions would be significantly impacted by massive power outages or failures of U.S. communications services. In addition to providing regular updates on the latest threat mitigation techniques, DHS released the *Banking and Finance Sector Specific Plan*[1] in 2007, which characterizes

[1] http://www.dhs.gov/files/programs/gc_1179866197607.shtm

vulnerabilities associated with links between financial institutions and other sectors while offering sector-specific risk considerations.

Though malicious cyber actors have varying levels of access and technical sophistication, all seek to inappropriately leverage the systems they target. Analysis of criminal activities shows increasing levels of sophistication in technical and targeting capabilities as well as a willingness to sell these capabilities on the black market. Some adversaries are capable of disrupting, destroying, or exploiting U.S. information systems including those that support the Banking and Finance Sector while others pursue intelligence collection, intellectual-property theft, monetary theft, and the disruption of commercial activities. In response to these growing and persistent threats, the Banking and Finance Sector has developed sophisticated tools and frameworks to defend against, detect, respond to, and mitigate cyber threats in collaboration with other stakeholders, including IT sector companies and experts who often provide these capabilities to the financial sector.

Additionally, the Federal government's unique expertise and ability to coordinate analytical and response activities among government, law enforcement, and the intelligence community complements the Banking and Finance Sector's efforts. Based on the framework established by the *National Infrastructure Protection Plan (NIPP)*, DHS collaborates with the U.S. Department of the Treasury (Treasury) as the Sector-Specific Agency for the Banking and Finance Sector, the Financial Services Sector Coordinating Council (FSSCC) for Critical Infrastructure Protection and Homeland Security, the Financial Services Information Sharing and Analysis Center (FS-ISAC), and other industry and interagency partners to reduce the risks posed to the critical systems that support the Nation's financial institutions. DHS also offers direct assistance to individual companies by assisting in analysis and improving their cybersecurity posture in addition to responding to requests for assistance from companies who have been compromised.

Despite significant outreach and relationship building, DHS faces a number of constraints in coordinating with the private sector, which may impact work with financial institutions. Some institutions have concerns about the privacy implications of sharing information with the Government or about brand damage that may result from reporting an incident. Through trusted relationships with financial sector institutions, including the Protected Critical Infrastructure Information program, DHS works to prevent inappropriate disclosure of proprietary information or other sensitive data. Furthermore, the Administration's cybersecurity legislative proposal offers a chance to provide clear statutory authority to facilitate greater information sharing between DHS and the private sector.

DHS Cybersecurity Mission

No single technology or government entity can overcome the cybersecurity challenges the Nation faces on its own. The public and private sectors must work collaboratively to address the risks posed to our Nation's critical systems.

At DHS's National Protection and Programs Directorate (NPPD), in addition to leading the effort to secure Federal Executive Branch civilian agencies' unclassified networks, we are responsible for several other cybersecurity missions, including:

- Providing technical expertise to the private sector and to critical infrastructure owners and operators, including at the state and local levels, in order to enhance their cybersecurity preparedness and broaden their risk assessment, mitigation, and incident response capabilities;
- Raising public cybersecurity awareness; and
- Coordinating the national mitigation response to cyber incidents.

In 2009, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated cyber activities should remain a priority for the federal government. Consistent with the CNCI's priorities, the President's *Cyberspace Policy Review* established a strategic framework for advancing the Nation's cybersecurity policies. Following the May 2009 publication of this review, DHS designated safeguarding and securing cyberspace as a priority mission area in the Quadrennial Homeland Security Review (QHSR). To execute on this mission area, DHS established the following two overarching goals:

- Creation of a safe, secure, and resilient cyber environment and
- Promotion of cybersecurity knowledge and innovation.

Within NPPD, the Office of Cybersecurity and Communications (CS&C) focuses on reducing the risks posed to communications and information technology infrastructures, and to the sectors that depend on those infrastructures. CS&C also seeks to enable timely response and recovery of these infrastructures in all circumstances while coordinating information sharing efforts among Federal law enforcement, intelligence, defense, and homeland security communities to ensure a common operating picture of the cybersecurity and communications environment. Three divisions make up CS&C: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System. In addition, CS&C established the National Cybersecurity and Communications Integration Center (NCCIC), which coordinates interagency mitigation response efforts in the event of a significant cybersecurity incident.

Consistent with its role in implementing the NIPP, NCSD collaborates with the Banking and Finance Sector to conduct risk assessments and mitigate vulnerabilities and threats capable of affecting the sector's information technology assets and critical infrastructure. NCSD's Cyber Security Evaluations Program conducts Cyber Resilience Reviews to proactively determine how various organizations manage the cybersecurity of significant information services and assets while offering guidance to improve cybersecurity management and reduce operational risks related to cybersecurity. In doing so, NCSD carries out the majority of DHS's non-law enforcement cybersecurity responsibilities within the financial services sector.

One of NCSD's operational arms, the U.S. Computer Emergency Readiness Team (US-CERT), works closely with banking and finance sector partners to provide analytical expertise and to share threat and vulnerability information in collaboration with other critical infrastructure sectors, law enforcement, and the intelligence community. Through the FS-ISAC, the Banking and Finance Sector provides US-CERT with threat, incident, and vulnerability data, which is then integrated into US-CERT's analytical and information sharing processes.

NCSD's Critical Infrastructure Cyber Protection & Awareness (CICPA) branch builds on this effort by providing security clearances to key cybersecurity officials within the Banking and Finance Sector. For example, DHS has sponsored Top Secret/SCI clearances for select members of the financial services sector and numerous Secret-level clearances in partnership with Treasury to broaden the scope of information that US-CERT can share. US-CERT has also benefits from close operational collaboration with DHS's U.S. Secret Service Criminal Investigative Division (USSS-CID), which has concurrent jurisdiction with the FBI over the investigation of computer crime and protects the Nation's financial payment systems while combating transnational financial crimes committed by terrorists and other criminals.

Research and Innovation

In addition to NPPD's cybersecurity activities, the DHS Science & Technology (S&T) Directorate is closely engaged with the Financial Services Sector. One of the many innovations emerging from S&T's partnership with the Financial Service Sector is the Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE) software suite. DECIDE will enable enterprise decision makers to evaluate responses to operational disruptions of market-based transactions across networks. This allows stakeholders to pursue effective business continuity practices that address increasingly sophisticated cyber threats. DHS Science & Technology (S&T) Directorate is closely engaged with the FSSCC to develop capabilities to protect citizens by enhancing the resilience, security, integrity, and accessibility of information systems used by financial institutions and other critical infrastructures. In December 2010, S&T signed a memorandum of understanding with the FSSCC and the National Institute of Standards and Technology (NIST) to expedite the coordinated development and availability of collaborative research, development, and testing activities for cybersecurity technologies and processes.

Interagency and Sector Coordination

The success of our efforts to reduce cybersecurity risks posed to the Banking and Finance Sector depends on effective communication and critical partnerships. No single entity has sole responsibility for securing cyberspace. To that end DHS works with its Federal partners to host a number of initiatives focused on enhancing coordination and information sharing with the private sector.

Private Sector Security Clearance Program

The NCCIC maintains a program that hosts Top Secret/SCI-cleared private sector representatives on the NCCIC operations floor including representatives from the FS-ISAC. This program was created to closely integrate the operational capabilities of the NCCIC, various critical infrastructure sectors, and individual companies. The FS-ISAC's presence on the NCCIC floor enhances the analysis, warning, and response capabilities associated with critical information systems and improves the overall cybersecurity of the Banking and Finance Sector and the Nation.

Cybersecurity Information Sharing and Collaboration Program

In February 2010, DHS, the Department of Defense, and the FS-ISAC launched a pilot designed to help protect key critical networks and infrastructure within the Banking and Finance Sector by sharing actionable information. Based on knowledge gained from the pilot, DHS is expanding

its information sharing and incident response coordination processes with other critical infrastructure sectors and leveraging capabilities from within DHS and across the response community. Specifically, DHS plans to launch the critical infrastructure Cybersecurity Information Sharing and Collaboration Program this year, which seeks to create a secure online collaboration portal where registered critical infrastructure sector entities can provide accurate, timely, and thorough information about current, emerging, and evolving threats posed to critical infrastructure networks. The portal will have the capability to process Protected Critical Infrastructure Information while offering timely and actionable analysis and mitigation products for critical infrastructure participants based on stakeholder contributions and unclassified government reporting.

Cyber Operations Resiliency Review Pilot Program
In addition, NCSD, in partnership with Treasury and the BITS Financial Services Roundtable, is implementing a two-phase pilot program to proactively assess the degree of cyber resilience and presence of malicious activity on up to five financial institutions' enterprise networks. In the first phase, analysts from CICPA's Cybersecurity Evaluation Program will measure the adoption and growth of cybersecurity risk management using a common capability-based evaluation framework. In the second phase, US-CERT will analyze institution-provided data for evidence of malicious activity. If malicious activity is found, US-CERT will provide the institution with targeted strategies to mitigate the activity and protect against similar activity in the future.

National Cyber Incident Response
The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." To address this presidential priority, DHS created a working group of stakeholders from the public and private sectors that drafted the *National Cyber Incident Response Plan* (NCIRP). The NCIRP provides a framework for the NCCIC's response capabilities and for coordination of Federal, state and local governments, the private sector, and international partners during significant cyber incidents. The plan specifically addresses the role of the Treasury and the FS-ISAC in providing for coordination of national response capabilities by providing flexible, adaptable synchronization of response activities across jurisdictional lines. In September 2010, DHS tested the NCIRP during a response exercise in which members of the domestic and international cyber incident response community addressed a scenario of a coordinated cyber event. The NCIRP working group is now completing the final stages of plan revision using observations from the exercise and experience from real world events.

National Strategy for Trusted Identities in Cyberspace
DHS also worked closely with our public and private sector partners on, the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC), which seeks to increase the security of online transactions through the development of more trustworthy digital credentials. The adoption of more trustworthy credentials will help to reduce account takeovers and raise overall consumer safety levels. Trusted identities are a key part of the Department's vision for a healthy cyber ecosystem. The voluntary adoption of credentials envisioned by the NSTIC will make online transactions faster, more convenient, safer and more private.

DHS Technical Assistance to the Banking and Finance Sector
Over the past year, DHS has demonstrated its ability to assist financial institutions with cyber intrusion mitigation and incident response while building on lessons learned. Initiating technical assistance with any private company to provide analysis and mitigation advice is a sensitive endeavor that requires trust and confidentiality.

In June 2010, for example, US-CERT partnered with the Federal Bureau of Investigation (FBI) to address a specific threat impacting a U.S. financial institution. By providing remote operational support following a formal request for technical assistance from the financial institution, US-CERT was able to analyze the threat, develop near-term mitigation recommendations, and identify strategies for preventing similar activity. In this instance, malicious actors used a combination of legitimate and illegitimate data to create false online accounts, ultimately giving them access to sensitive systems. A rapid cross-sector and interagency response effort prevented any known financial losses from this event.

As a result of knowledge gained during this engagement and from the collaborative relationship built with this particular financial institution, US-CERT was better able to assist another financial institution that experienced a similar event. In June 2011, US-CERT partnered with the Secret Service to assist the second institution with their detection and mitigation efforts and leveraged its relationship with the initial institution to bring the two entities together to discuss the vulnerability.

During an unrelated event in December 2010, US-CERT partnered with FBI and the National Security Agency to provide on-site and remote assistance and support in response to a significant cybersecurity incident involving financial entities. Upon formal request, US-CERT was able respond to this incident with specialized technical insight, support, and assistance. Specifically, US-CERT conducted interviews and briefings with high-ranking company officials, served as the lead for a skilled technical team of network analysts, and coordinated the development of a mitigation strategy with other agencies and financial sector institutions. Through our analysis and unique capability to coordinate cross-sector and interagency response efforts, we discovered other potential and actual victims of this threat. US-CERT aggressively worked to publish alert and awareness products for the wider community.

Of course, these are just two examples of how DHS works to achieve success in the analysis and warning mission space. We have proven our ability to earn stakeholder confidence when it comes to mitigating threats posed to networks, to reduce future risks, and to serve as the Federal government's focal point for analyzing incident reports.

Conclusion
The Nation's cybersecurity activities are set in an environment characterized by a combination of known and unknown vulnerabilities, rapidly expanding capabilities, and challenges in maintaining comprehensive threat and vulnerability awareness. The mission to reduce the cyber risks posed to the Banking and Finance Sector's critical systems is a national endeavor, requiring broad collaboration. Robust public-private approaches to cybersecurity are essential to ensuring that government, business, and the public can continue to use the critical services on which they depend. DHS is committed to working with its partners to create a safe, secure, and resilient

cyber environment that supports the Banking and Finance Sector and fosters national economic prosperity.

Thank you for the opportunity to discuss emerging issues in cybersecurity with you today and I am pleased to answer any questions you might have.

House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
September 14, 2011
Testimony of Dr. Gregory E. Shannon
Software Engineering Institute
Chief Scientist for the CERT Program

Chairwoman Capito, Ranking Member Maloney, and other distinguished Members of the Subcommittee on Financial Institutions and Consumer Credit, thank you for the opportunity to come before the Subcommittee to testify, it is my pleasure to be here this morning to discuss the cyber threat to financial institutions.

About CERT®

The CERT Program is part of Carnegie Mellon University's Software Engineering Institute (SEI), a Department of Defense Federally Funded Research and Development Center (FFRDC), and is located on the Carnegie Mellon campus in Pittsburgh, Pennsylvania.

The CERT program (http://www.cert.org/) has evolved from the first computer emergency response team created by the SEI, at the request of Department of Defense Advanced Research Program Activity (DARPA), in 1988 as a direct response to the Morris worm incident. The CERT program continues to research, develop, and promote the use of appropriate technology and systems management practices to resist attacks on networked systems, limit damage, restore continuity of critical systems services, and investigate methods and root causes. CERT works to mitigate both cyber risks and facilitate local, national and international cyber incident responses. Over the past 23 years CERT has led efforts to establish over 200 CERT computer security incident response teams (CSIRTs) around the world – including the Department of Homeland Security (DHS) US-CERT. We have proven track record of success in transitioning research and technology to those who can implement it on a national scale.

Dr. Greg Shannon is the Chief Scientist for the CERT Program, where he leads technology innovation efforts to establish and enhance the CERT program's research, development and strategic policy initiatives.

Understanding today's cyber threats is more than just war stories, anecdotes and scare tactics. The threat is real, it is now, and it is evolving; CERT catalogues ~250,000 instances of candidate malware artifacts each month. At this volume is difficult to determine in real time which are malicious, let alone what their intent. Unsurprisingly, the limit in our technical abilities to provide security has brought about the steady corporatization of the cyber security threat. Cyber attacks have become big business, with extraordinary returns on investment; for example, botnets are both economical and flexible for creating cyber effects at scale, including attacks on financial institutions and their customers, which yield high payouts.

To efficiently fight the cyber threat we need realistic outcome based solutions, enabled by a data driven approach to research, development, policies and regulations. There is an emerging

science of cyber security, and I encourage the Subcommittee to support practices that are both scientifically and operationally validated as part of a continuing dialogue on important policy discussions. CERT is working with both U.S. Government Agencies and the Financial Community to help limit the Nation's exposure to cyber attacks, but more can be done. The U.S. Government and the globalized Financial Sector need computing infrastructure that is more secure *and* more resilient in order to mitigate the escalating threats. Filling the technological gaps in current forensic abilities as well as augmented capabilities to locate the source of the attack and limit the damage are much needed. Finally, leadership and support from the government in policy discussions that bring focus and funding for more robust research in key areas of cyber security, is essential.

Examining the Threat – from the Inside

While there are many methods to launch a cyber attack on the financial sector, I would like to highlight the risks of insider threats. CERT is using incident case data in combination with hands-on collaboration with practitioners in industry and government to understand how best to mitigate insider threats.

The continued stress of the current economy on the workplace is impacting and exacerbating the potential for insider threat. Organizations are working hard to build walls around their network infrastructure to keep people out but are having a difficult time defending against potential menaces that are already on the inside of the fence.

I am going to highlight some areas of concern that we have been focused on at the SEI. These points present a general picture of the problem:

- According to our data, over the past 7 years malicious insider attacks have affected approximately half of all organizations.
- CERT's data also reveals that the insider threat is not limited to rogue individuals acting alone, but rather, almost half of all malicious insiders in the Financial Services industry colluded with outside conspirators, while a third recruited other insiders to carry out their crimes.
- In CERT's research, we discovered that around 10% of fraud cases involved organized crime; average losses in those cases were $4 million.
- Other complexities include trusted business partners (e.g. outsourcing), mergers and acquisitions, and branches located outside of the US. This exacerbates the problem due to cultural issues, national loyalties, and legal issues such as more stringent employee privacy laws.

Insider crimes in the financial services sector are not limited to fraud, but also include theft of intellectual property and insider IT sabotage. One former system administrator wiped out billions of files on a financial institution's servers all over the world at 9AM one morning; and recently an individual copied source code containing proprietary trading algorithms to servers outside the U.S. after submitting his letter of resignation.

Although there are a vast number of cybersecurity tools available, most are used on protection from breaches from outside. The difficulty in creating effective automated tools for detection

from insider threats is that malicious insiders typically commit their illicit activity by performing the same types of online actions they do every day, only with malicious intent. In fact, insider fraud is often detected either through traditional auditing methods or discovery by external parties, such as customers.

CERT's work in this area began in 2001, through the support of the United States Secret Service. Over the past 10 years CERT has collected and rigorously analyzed over 700 actual cases of insider crimes spanning all critical infrastructure sectors. Within that sample, there were 147 cases involving the financial services sector. We use these cases for research and analysis, and produced models, best practices, and training for government and industry on prevention and detection of insider threat. A crucial part of CERT's research mission is to make the most of the data we have, to use insightful statistical analysis to understand the breadth of the problem and solutions, and to seek out additional highly-informative sources of data to improve our research, results and impact.

Within the past 3 years two different divisions of DHS sponsored the SEI to enhance our understanding of the insider threat problem and to make recommendations aimed at building new solutions that would be readily available to the Community. CERT recommended using existing technology that most organizations already have in place as the platform for our solutions; the first set of controls will be published and made available to the public this month. We have also developed an insider threat assessment framework, which CERT is piloting with federal agencies, to identify vulnerabilities to insider threat. This will enable CERT to provide recommendations for both the government and industry to use as benchmarks for insider threat defenses. In addition, we are building a training and certification program so that organizations can assess their own vulnerabilities to insider threats. This work is being sponsored by DHS National Cybersecurity Division Federal Network Security Branch.

CERT has also been working with the Secret Service, the Financial Services sector, and the Department of Treasury, sponsored by DHS Science and Technology, to build a model of insider threat specifically for fraud within the financial sector. As an FFRDC, CERT is able to work across the government and the private sector to ensure our research successfully transitions into operationally viable solutions for the nation, and then offer those best of breed solutions to the community at large. CERT has built a relationship throughout the financial community, including the BITS Fraud Steering Committee and the FS-ISAC to create a direct feedback loop of information and data sharing so that we can validate our models and then provide both industry and government with the methods and tools they need to combat the mounting problem.

Building More Secure Systems - Secure Coding

Software vulnerability reports continue to grow at an alarming rate, and a significant number of these reports produce technical security alerts. To address this growing threat to governments, corporations, educational institutions, and individuals, systems must be developed that are free of software vulnerabilities.

CERT takes a comprehensive approach to eliminating vulnerabilities and other software defects, starting with a detailed analysis of vulnerability reports originating from the U.S. Department of

Defense (DoD) and other sources. By analyzing thousands of vulnerability reports, CERT has observed that most vulnerabilities stem from a relatively small number of common programming errors. Software developers can take practical steps to eliminate known code-related vulnerabilities by identifying insecure coding practices and developing secure alternatives.

These new coding standards, developed in coordination with security researchers, language experts, and software developers using a wiki-based community process (More than 500 contributors and reviewers participated in the development of secure coding standards on the CERT® Secure Coding Standards wiki.[1]) encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, rather than by the programmer's familiarity or preference. Moreover, they provide a metric for evaluating and contrasting software security, safety, reliability, and related properties; and when applied during software development these coding standards can create more secure systems.

Resilience

Operational Resilience is a new discipline that blends computer security with business risk management; and is the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner. In 2004, CERT began a partnership with the Financial Services Technology Consortium (www.fstc.org) to examine the application of survivability concepts to the complex problem of managing operational resilience in the U. S. financial sector. Due to CERT's trusted relationship we are given unparalleled access to some of the best practitioners in the security and business continuity space.

The focus is not only to thwart computer intruders, but also to ensure that business goals are met and critical business functions are sustained despite the presence of cyber attacks. Improving survivability in the presence of cyber attacks also improves the ability of business to survive accidents and system failures that are not malicious. Resilience depends on three key capabilities: resistance, recognition, and recovery. Resistance is the capability of a system to repel attacks. Recognition is the capability to detect attacks as they occur and to evaluate the extent of damage and compromise. Recovery, a hallmark of survivability, is the capability to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack.

Through our collaboration with the FSTC (FSTC has since been incorporated into BITS as part of the Financial Services Roundtable), as well as from extensive review of existing codes of practice in the areas of security, business continuity, and IT operations management, CERT codified a draft process definition for operational resilience management processes called the CERT Resilience Management Model (RMM). Recently, CERT was asked to participate in the Payment Risk Committee's Executive Seminar on Business Continuity and Resilience Planning: A Decade After 9/11 at the Federal Reserve Bank of New York, to speak about the RMM, in our speech on "Resilience Management: Ensuring Sufficient Forethought." Building on the success of previous work in the financial sector, CERT is currently conducting a year-long resilience improvement workshop series with members of the defense industrial base, financial services,

[1] https://www.securecoding.cert.org

government, and academic communities. As a result of the success of this workshop series, CERT is currently in the planning stages with major financial institutions to begin a series of workshops focused on the Financial Services Industry using the CERT Resilience Management Model and the Insider Threat Assessment Methods to craft an improvement path for managing operational risk from incidents, insiders, and external events. In addition, through these workshops CERT is making major inroads in developing and piloting measures that can be used to verify that organizations have indeed become more operationally resilient as a result of the controls, practices, and processes they are implementing and sustaining. Participants in current CERT-RMM workshops are piloting and testing these measures as a way to evolve their security and continuity programs away from mere compliance activities toward verification and validation activities.

Forensics

Computers are no longer just the targets of crime; our adversaries now use them to facilitate every aspect of their illicit activities and achieve effects at scale. Once an incident occurs the federal government and the financial community face several hurdles to recover the needed data in order to locate the source of the incidents and contain the problem.

First, computer forensic labs are constrained by a lack of resources, creating an enormous backlog rendering them unable to handle the mega-fold increases in the volumes of data that need to be examined for evidence. When an intrusion into a financial institutions network occurs, time is crucial, immediate decisions are required to deal with instant consequences as well as longer-term consequences (like prosecution of a case). While some entities may have the qualified examiners, and many do not, they lack the funds to properly equip them for the mission. For example, current examination methods rely heavily on processor power, but due to dramatically increased computer memory, examination stations often cannot keep up. Finally, the current state of the practice does not allow examiners to easily access varied levels of expertise in a timely or cost-effective way, resulting in time delays and increased costs.

To successfully respond to cyber incidents these obstacles must be overcome in a way that allows for high-quality, expedited collaborative examinations. For instance, what would happen if an adversary perpetrated an actual, severe cyber event on the financial sector with national consequences? Currently, there is no one facility or lab that could support the volume of data these kinds of events would generate. Under current conditions, data would have to be distributed, adding to the time and complexity of conducting examinations. Analysts and investigators will need flexible, secure access to high-performance systems, to increase productivity and facilitate effective distributed collaboration in a scalable and cost- effective way. Additionally, to support better response, security, privacy and resilience organizations must design and architect their processes and systems in line with scalable assurance principles developed at the SEI and in the broader software and systems engineering communities.

To enable organizations to accelerate the tempo of their investigations CERT is working on a new incident analysis framework which speeds up the velocity of investigation and allows for a faster and adaptive defense and mitigation opportunities otherwise not available in near real-time. To help augment the cyber forensic capabilities of law enforcement the CERT program

created the Clustered-Computing Analysis Platform (C-CAP). C-CAP is designed to support 200 concurrent computer examinations looking at 200 terabytes of data, allowing for a massive, coordinated effort. Absent catastrophic events, the C-CAP environment can offer underequipped or overwhelmed agencies real time additional resources. C-CAP is a state-of-the-art forensics analysis environment that provides a complete suite of tools for host-based and network investigations. C-CAP augments scarce resources by allowing multiple users to view the same data, either remotely or locally; while maximizing the application of specialized computing resources to the forensic and incident response missions. Analysts and investigators enjoy flexible, secure access to high-performance systems, increasing productivity and facilitating distributed collaboration. Designed specifically for forensics and incident response analysis, this unique integration and packaging of tools, accelerates the analysis processes, maximizes performance and reduces costs. C-CAP is a flexible solution, allowing agencies to add or remove components that are relevant to their particular needs. Its unique centralized management interface allows organizations to rapidly allocate platform resources to tasks or analysts. Scalable and cost-effective, C-CAP can be customized to suit any organization, regardless of size and mission.

More Robust Research Agenda

Research is only as good as the data it is created from, and currently researchers have limited access to data, resulting in sub-par solutions and stifling innovation. To truly begin to combat the cyber threat we must gain better situational awareness, and it is the federal government's role to generate situational awareness beyond what any private entity has the incentive to produce. However, achieving this enhanced situational awareness will require continued research on network traffic and data and the cooperation of the financial community.

Richer data needs to be shared with the research community, not only incident data itself, but also data-sets that will enable an understanding of what "normal" resembles, enabling the detection of malicious markers that are invariant, such as behavioral based indicators (e.g. insider threats). Currently, there is not a clear understanding of what this data set would look like; but if situational awareness is to develop beyond simple indicators, the financial sector must allow access to everyday data, so that researchers can begin to recognize what data sets are important.

This data sharing should start with limited access to high-fidelity datasets for researchers so that data with scientifically proven value is considered for sharing operationally. Otherwise, policymakers and experts are left to speculate what is the right data to share. Furthermore, if the research community was able to successfully determine which data sets where imperative to combating the cyber threat, then in effect less data would need to be shared to productively handle cyber dangers.

However, I realize information sharing on this scale tends to exacerbate an already contentious relationship between security and privacy. Security and privacy advocates often are at odds with one other in discussions of how security degrades privacy or privacy degrades security. This is an unhealthy condition, and our adversaries are exploiting it and degrading cyber space for us all. Privacy advocates contend without privacy there is no security. But given our ever more

interconnected world the loss of anonymity is unavoidable, and I believe that without security there is no privacy.

Lastly, the government in collaboration with the financial sector needs to encourage and enable more research to be done in the areas of identity management and authentication. As banking becomes more and more mobile, at the demand of the consumer, we need better ways to secure our data while preserving a user-friendly platform.

Conclusion

I cannot end my testimony without saying something about the need for a robust cyber workforce. An educated and equipped workforce is essential to handling the cyber threat to financial institutions. However, the rapid changes and dynamic nature of cybersecurity make keeping the workforce up to date a very challenging problem. The most common workforce development training solution is the traditional classroom training model. While this training model is easy to implement and is widely used, there are a number of reasons it is not adequate for providing effective, large-scale training to a technical workforce including time, cost and scalability. CERT uses innovative platforms for the federal workforce and these models, such as CERT's Virtual Training Environment (VTE) or Exercise Network (XNET), could be emulated to successfully train cyber professionals within the financial community

In conclusion, good cyber security must be built on scientifically sound research and operationally valid data. I have shown where CERT successfully applies these approaches. I believe that such well-founded security enhances privacy. I encourage the Subcommittee to consider policies that promote other such "dual" impact cyber security R&D. If the subcommittee can foster access to data for scientifically valid research, I believe that not only will research be better, but policy makers will have better information for making regulatory decisions. I hope the Subcommittee will encourage policy and research discussions between the security and privacy communities; we all would benefit with improved cyber security and privacy.

Appendix A

Insider Threat Blog
http://www.cert.org/blogs/insider_threat/2010/12/case_trends_for_type_and_status_of_insiders.html

Insider Threat Case Trends for Employee Type and Employment Status
By Insider Threat Team on December 21, 2010 10:45 AM |

We recently met with leaders from the U.S. financial services sector, and they asked a number of questions about recent trends in insider threat activities. We are often asked these types of questions, and we can answer many of them right away. Others require more extensive data mining in our case database. In this entry, we address the following question:

Between current employees, former employees, and contractors, is one group most likely to commit these crimes?

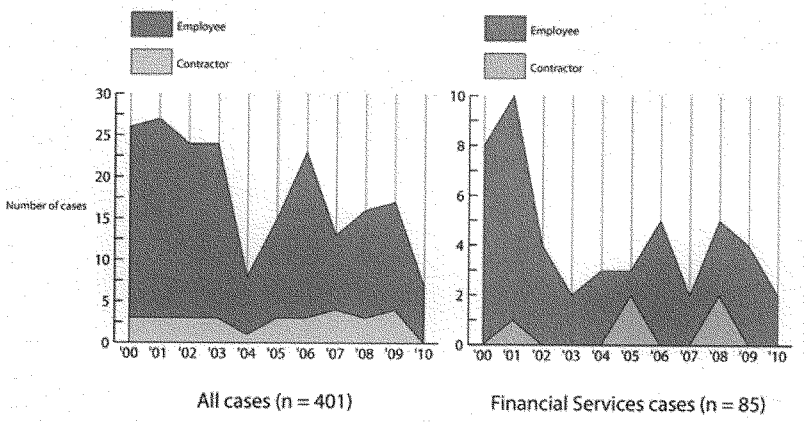
The answer to this question has some important implications, and not just for these particular meeting attendees. If, across all types of incidents and all sectors, the vast majority of incidents are caused by current, full-time employees, organizations may focus on that group to address the vulnerability. If, on the other hand, there are a large number of part-time contractors or former employees, there may be different controls that an organization should consider using.

Before we discuss the data and its implications, there are some caveats. Our sample of incidents only involves individuals who were caught and prosecuted for their crimes. Also, we currently only have data about incidents that were reported to law enforcement, so these were examples that reached a certain threshold of damages and satisfactory evidence to furnish in a court of law. Finally, it is not entirely accurate to infer from our sample that the results and figures apply to all sectors and all organizations. We are providing these statistics as "food for thought" and to add to the discussion about an important threat that most organizations face.

To develop the answer to the question above, we used 401 cases of all crime types (i.e., IT sabotage, fraud, and theft of intellectual property) spanning all critical infrastructure sectors. Within that sample, there were 85 cases of all types of crime involving only the financial services sector.

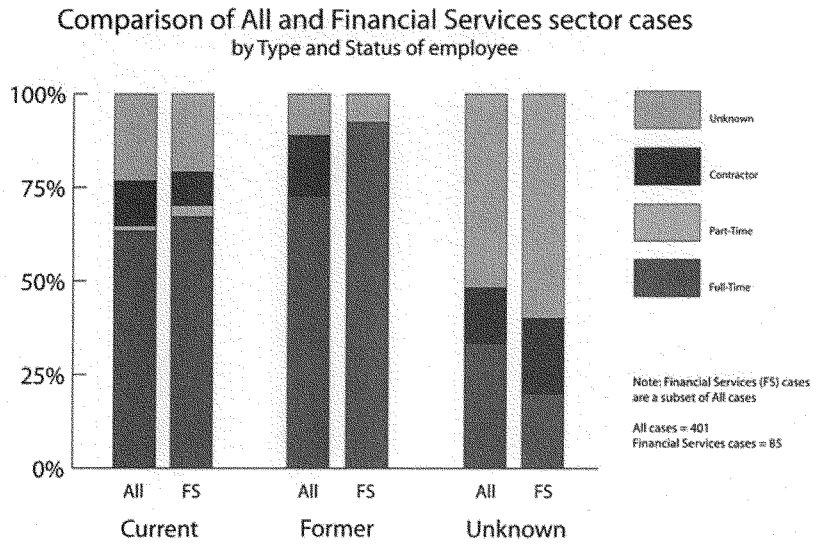
The figure below shows the number of cases per year by employee type, constrained to either employee (current or former) or contractor. The graph on the left shows all cases, while the one on the right shows only financial services sector cases.

Comparison of All and Financial Services sector cases
by type of employee over time



In the ten years shown in the graphs, the percentage of incidents involving a contractor hovers around 15%. Whether the number of total incidents for a particular year is higher or lower, the percentages stay roughly the same. What is most interesting about these two graphs is that this ratio has stayed the same over the course of ten years of a fairly tumultuous economic environment. This result may indicate that it isn't likely for contractor crimes to raise or lower significantly. But with almost 1 in 7 of our insider threat crimes being committed by contractors, are organizations adequately considering the risk posed by this group?

The second figure below shows the percentage of cases perpetrated by current and former employees in all cases and in only the financial services sector. The chart also shows the ratio of employment type (full-time, part-time, or contractor) depicted within each bar. In some cases, we were not certain whether the incident was committed by a current or former employee, so we indicated those incidents as unknown.



At first glance, the financial services sector cases seem to mirror all cases. Full-time employees have the greatest percentage across all sectors for both current and former employees. Part-time employees form a small percentage of our cases across all employee status and types. The contractor results, on the other hand, reveal an interesting trend. For current employees, the percentage is about the same for financial services as all sectors. For former employees, however, 16% of all cases were contractors (indicated in burgundy in the center-left bar), and none of those were in the financial services sector.

These results may be meaningful or may be an artifact of the small number of cases (only 16) of former employees in the financial services sector. Regardless, these graphs provide some interesting data points for you to examine within the context of your own organization. Do you use the same prevention and detection controls for all employees, or are you only worried about the majority—the current, full-time employees you see on a daily basis? Use the feedback link to send us your thoughts.

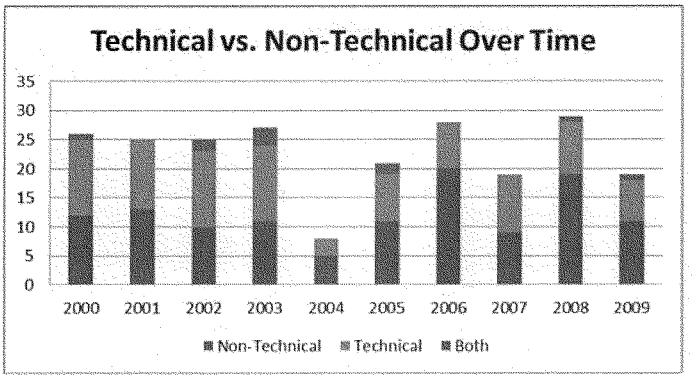
Insider Threat Case Trends of Technical and Non-Technical Employees
By Insider Threat Team on January 26, 2011 10:08 AM |
http://www.cert.org/blogs/insider_threat/2011/01/insider_threat_case_trends_of_technical_and_non-technical_employees.html

This is the second of two blog entries that explore questions we were asked during a recent meeting with leaders from the U.S. financial services sector. In this entry, we focus on what role malicious insiders typically hold in an organization: a non-technical position, a technical position, or both. "Non-technical" includes positions such as management, sales, and auditors. "Technical" includes positions such as system or database administrators, programmers, and helpdesk employees. "Both" includes overlapping jobs such as IT managers.

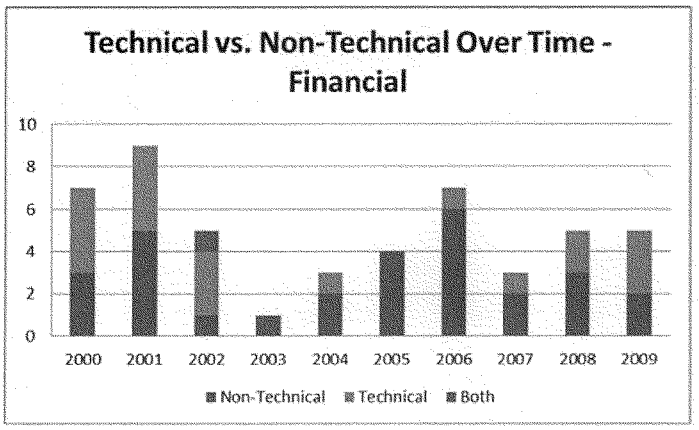
The statistics in this entry were generated from the cases that we have collected and observed. Your organization may see a very different breakdown of the positions held by malicious insiders, especially if you have a different allocation of technical and non-technical positions.

In our repository, we have data about the organizational position for perpetrators of 355 malicious insider incidents. Of those cases, 54% held non-technical positions, 41% held technical positions, and 5% held both. Looking specifically at the banking and finance sector, we had employment data for 73 incidents. Of those cases, 66% held non-technical positions, 33% held technical positions, and only 1% held both. It is interesting to note that we did not observe a drastic difference between the position breakdown in the banking and finance incidents and in our larger sample of cases. However, the results do seem to indicate that the majority of crimes that we have observed in banking and finance involve insiders in non-technical positions. If we examine the type of crime for all malicious insider incidents, 40% of the cases are fraud. Within only the banking and finance incidents, the percent of fraud cases increases to 70%. Our research indicates that non-technical employees perpetrate the majority of insider fraud crimes, so the difference in number of fraud cases may account for the increased percentage of non-technical positions within the banking and finance sector.

We also collect data on when the crimes occur, so we can compare technical versus non-technical crimes over the last ten years. Incidents that occurred in 2010 may still be reported, so we did not include 2010 in these graphs. The first graph includes all incidents where we knew the start date of the incident.



The next graph only includes financial sector incidents where we knew the start date of the incident.



Looking at the graphs, the ebb and flow of technical versus non-technical insiders could follow U.S. economic indicators. The steady increase in non-technical crimes leading up to 2006 in both graphs may coincide with the U.S. economic downturn. Are there other possibilities? Maybe one of you in the financial service sector can compare our timeline of incidents (from this blog entry and our previous blog entry) to some meaningful measures of the U.S. economy or to other general indicators of employee well-being?

Another aspect of this issue is whether damages differ between incidents involving technical versus non-technical insiders. For example, would technical insiders have more access to IT systems and therefore be able to cause more damage? Or would non-technical insiders with

much more restricted access but more knowledge of the data in the systems be able to cause more damage? Before we answer these questions, keep in mind that, for now, our case repository only includes cases that organizations report to law enforcement. Therefore, our data might exclude lower damage incidents that organizations handle internally.

In our repository, the average impact between technical and non-technical cases in the financial services sector is relatively similar. The average damages for our technical cases were more than $750,000. The average damages for our non-technical insiders were more than $800,000. (Note: The average value for non-technical incidents does exclude one outlier case of a theft that spanned several years and resulted in almost $700,000,000 worth of damages.)

How has your organization allocated resources for preventing, detecting, and responding to threats posed by technical and non-technical employees? Does your organization focus on one type of employee and not the other? Our observations indicate that there is not a substantial difference between organizational roles of malicious insiders, so organizations must consider each category of employee when implementing security controls. Insider threat could come from anyone.

As always, we welcome your feedback.

Statement of

A.T. Smith
Assistant Director
U.S. Secret Service

Hearing before the
House Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

"Cyber Security Threats to the Financial Sector"

September 14, 2011

Good morning Madam Chair, Ranking Member Maloney and distinguished members of the Subcommittee. Thank you for the opportunity to testify on U.S. Secret Service's (Secret Service) investigative role in combating cyber crime.

As the original guardian of the Nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

In 2010, the Secret Service's unique multifaceted approach to combating cyber crime led to the arrest of over 1,200 suspects for cyber crime related violations and the examination of 867 terabytes of data. To put it in perspective, that is nearly four times the amount of data collected in the archives of the Library of Congress[1]. These investigations involved over $500 million in actual fraud loss and prevented approximately $7 billion in additional losses. As a result of our efforts, the Secret Service is recognized worldwide for our innovative approaches to detecting, investigating and preventing cyber crimes. Furthermore, in alignment with the President's Comprehensive National Cyber Security Initiative, the Secret Service will continue to raise our overall capabilities in combating cyber crime and related forms of illegal computer activity.

---

[1] U.S. Library of Congress. (n.d.) *Library of Congress: Web Archiving FAQs.* Retrieved from http://www.loc.gov/webarchiving/faq.html#faqs_05.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, development and use of malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. As large companies have adopted more sophisticated protections against cyber-crime, criminals have adapted as well by increasing their attacks against small and medium-sized businesses, banks, and data processors. Unfortunately, many smaller businesses do not have the resources to adopt and continuously upgrade the sophisticated protections needed to safeguard data from being compromised.

The Secret Service has continued its collaboration with Verizon on the 2011 Data Breach Investigations Report (DBIR) to identify emerging threats, educate Internet users, and evaluate new technologies that work to prevent and mitigate attacks against critical computer networks. Researchers from law enforcement and the private sector examined roughly 800 new data breaches. The results from the Verizon study show that two of the noticeable trends in cybercrime over the past couple of years involve the ongoing targeting of Point of Sale (POS) systems as well as the compromise of online financial accounts, often through malware written explicitly for that purpose, with subsequent transaction fraud involving those accounts.

Compared to recent history, it appears that while there were more data breaches in 2010, the amount of compromised data decreased due to the size of the compromised companies' databases. This change may indicate that organized cybercriminals are becoming more willing to go after the smaller, easier targets that provide a smaller, yet steady, stream of potentially available data. In light of recent arrests and prosecutions following large-scale intrusions into financial services firms, criminals may be weighing the reward versus the risk, and opting to "play it safe".

The report also indicates that there has been a noticeable increase in account takeovers that result in fraudulent transfers from the victim's account to an account under the control of the perpetrator. This increase can be directly tied to the continued rise of malware variants created to capture login credentials to financial websites. The Secret Service and the financial services community are working together to combat this growing trend. The Financial Services Information Sharing and Analysis Center (FS-ISAC) has teamed up with the Secret Service, Department of the Treasury, Department of Justice and the FBI, and many other agencies to create the Account Takeover Task Force (ATOTF), which focuses on prevention, detection and response to account takeovers.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding forums," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites

vary in size; some of these criminal forums are limited to a few hundred members while others boast memberships of tens of thousands of users. Within these portals, there are separate forums moderated by senior and experienced members of the carding community who discuss tactics and techniques for overcoming security controls and pursuing complex fraud schemes. Criminal purveyors on these forums buy, sell, and trade malicious software, spamming services, credit and debit card data, personal identification data, bank account information, brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

Collaboration with Other Federal Agencies and International Law Enforcement

Cyber criminals may operate in a world without borders; however, the law enforcement community is constrained by jurisdictional boundaries. The successful investigation and adjudication of these transnational cyber crime cases is time and resource intensive.

In order to successfully perform its protective and investigative responsibilities, the Secret Service has cultivated relationships with state, local, and foreign law enforcement. Its domestic and international offices continue to serve as the platform from which the Secret Service expands its network of partners. The success of this approach is seen in a number of cases including the Secret Service's investigations into the complex network intrusions of TJX and Heartland Payment Systems – two of the largest data breach investigations ever prosecuted in the United States.

In addition, the Secret Service has been responsible for apprehending members of foreign organized criminal groups, such as the CarderPlanet criminal organization, that target the U.S. financial infrastructure through online intrusions and theft and exploitation of stolen financial information. Through extensive work and international coordination, the Secret Service was able to apprehend:

- A pioneer in the criminal world for developing a model in which he hired teams of hackers to target the financial industry to harvest card track data by the millions.
- A criminal who targeted home equity lines of credit maintained by persons on the list of wealthiest Americans. After traveling to the United States from his home in Russia he was apprehended and subsequently admitted to stealing millions of dollars.
- A co-founder of CarderPlanet, who also appears to have a background in law enforcement. The suspect is alleged to have created the first fully automated online store for selling stolen credit card data. Working with our international law enforcement partners, the suspect was identified and apprehended as he was boarding an international flight to Russia.
- A criminal who ran a variety of schemes with his partners in the former Soviet states while residing in Southern California. He is currently facing an array of charges in California.
- A criminal whose trafficking in stolen financial information was so brazen that Russian authorities worked with the Secret Service to secure a six-year prison sentence for the suspect in the Russian Federation.

The Secret Service, in conjunction with its many law enforcement partners across the United States and around the world, continues to successfully combat these crimes by adapting our investigative methodologies. Our success is due in part to the cooperation of these partners in more than a dozen international law enforcement agencies.

Currently, the Secret Service operates 24 offices abroad, including one in Beijing, China, which recently opened on September 11, 2011. While each office has regional responsibilities to provide global coverage, the personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), a key partner in preventing, investigating and prosecuting computer crimes. The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, and have resulted in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, and TJX and Heartland investigations, were a result of this valued partnership.

Mitigation and prevention are keys to reducing the threat from cyber criminals. Recognizing this reality, the Secret Service has strengthened its partnership and collaboration with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IP addresses and other information through its criminal investigations, it shares this information with US-CERT. To support such collaboration, US-CERT recently published Early Warning Indicator Notices (EWINs) on information gathered through Secret Service investigations. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

Secret Service Framework

In line with the Department's focus of creating a safer cyber environment and in order to protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- providing computer-based training to enhance the investigative skills of special agents through our Electronic Crimes Special Agent Program, and to our state and local law enforcement partners through the National Computer Forensics Institute;

- collaborating with our partners in law enforcement, the private sector and academia through our 31 Electronic Crimes Task Forces;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our Cyber Intelligence Section;
- maximizing partnerships with international law enforcement counterparts through our 142 domestic and 24 international field offices; and
- maximizing technical support, research and development in part with DHS Science and Technology Directorate, and public outreach through the Software Engineering Institute/CERT Liaison Program at Carnegie Mellon University and the Cell Phone/PDA Forensic Facility at University of Tulsa.

Electronic Crimes Task Forces

In 1995, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress further directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama and the Alabama District Attorney's Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Conclusion

As more information is stored in cyberspace, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line

of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations.

The Secret Service is committed to safeguarding the nation's financial payment systems. Responding to the increase in cyber crime and the growing level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, remaining innovative in it approach, providing training for law enforcement partners and raising public awareness.

Madam Chair, Ranking Member Maloney, and distinguished members of the Subcommittee, 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.

Department of Justice

STATEMENT OF

GORDON M. SNOW
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT

ENTITLED

"CYBER SECURITY: THREATS TO THE FINANCIAL SECTOR"

PRESENTED

September 14, 2011

Good afternoon Chairman Capito, Ranking Member Maloney, and members of the Subcommittee. I'm pleased to appear before you today to discuss the cyber threats facing our nation and how the FBI and our partners are working together to protect the financial sector and American consumers.

Cyber criminals can significantly threaten the finances and reputations of United States (U.S.) businesses and financial institutions. Given the abundance of potential victims and profits, cyber criminals will likely continue to target these entities. The FBI is committed to addressing these threats through innovative and proactive means and making the Internet more secure for financial institutions and U.S. consumers alike.

The Cyber Threat to the Financial Sector

As the Subcommittee is aware, the number and sophistication of malicious incidents has increased dramatically over the past five years and is expected to continue to grow. As business and financial institutions continue to adopt Internet-based commerce systems, the opportunities for cyber crime increase at retail and consumer levels.

Account Takeovers

Cyber criminals have demonstrated their abilities to exploit our online financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. In these instances, cyber crime is easily committed by exploiting the system users, rather than the systems themselves. This is typically done through the compromise of a legitimate user's account credentials.

Fraudulent monetary transfers and counterfeiting of stored value cards are the most common result of exploits against financial institutions, payment processors, and merchants. While the losses that result from these exploits generally fall upon the financial institution, consumers experience the inconvenience of changing accounts and replacing cards associated with their compromised information, as well as the emotional impact associated with being a victim of a cyber crime.

The FBI is currently investigating over 400 reported cases of corporate account takeovers in which cyber criminals have initiated unauthorized ACH and wire transfers from the bank accounts of U.S. businesses. These cases involve the attempted theft of over $255 million and have resulted in the actual loss of approximately $85 million.

Often, the attack vector is a targeted phishing e-mail that contains either an infected file or a link to an infected website. The e-mail recipient is generally a person within a targeted company who can initiate fund transfers on behalf of the business or another valid online banking credential account holder. Once the recipient opens the attachment or navigates to the website, malware is installed on the user's computer, which often includes a keylogging program that harvests the user's online banking credentials.

The criminal then either creates another account or directly initiates a funds transfer

masquerading as the legitimate user. The stolen funds are often then transferred overseas. Victims of this type of scheme have included small and medium-sized business, local governments, school districts, and health care service providers.

In 2008, a Pennsylvania school district discovered that over $450,000 was missing from their bank account. The following year, a New York school district reported that approximately $3 million had been transferred out of their bank account. The New York's school district's bank was able to recover some of the transfers, but $500,000 had already been withdrawn from the account before the transaction could be reversed.

Recently, two trucking companies were victimized by fraudulent electronic account transfers, and lost approximately $115,000. Compared to some loss figures, this might not seem significant. One of the companies currently has annual revenues worth roughly $79 million, so their loss was nearly .1% of their gross revenue. That amount is approximately enough to purchase an additional tractor-trailer and provide another driver with a job.

In March 2010, an Illinois town was the victim of a cyber intrusion resulting in unauthorized ACH transfers totaling $100,000. When an authorized individual logged into the town's bank account, the individual was redirected to a site alerting her that the bank's website was experiencing technical difficulties. During this redirection, the criminal used the victim's authorized credentials to initiate transactions. The town was able to recover only $30,000.

Third Party Payment Processor Breaches

Sophisticated cyber criminals are also targeting the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personally identifiable information (PII) of millions of individuals.

In November 2008, a U.S. payment processor discovered that hackers had breached the company's computer systems and compromised the personal data of over 1.5 million customers; roughly 1.1 million social security numbers were also exposed. The criminals used the stolen data to create fake debit cards and withdrew more than $9 million from Automated Teller Machines (ATMs) worldwide.

In January 2009, it was discovered that cyber criminals compromised the computer network of a U.S. payment processor that completes approximately 100 million transactions monthly for more than 250,000 U.S. businesses. The criminals were able to obtain over 130 million customer records, which included credit card numbers, expiration dates, and internal bank codes.

Securities and Market Trading Exploitation

Securities and brokerage firms and their customers are common targets of cyber

criminals. The typical crimes against these firms include market manipulation schemes and unauthorized stock trading.

In 2010, law enforcement agencies and financial regulators observed a trend in which cyber criminals initiated unauthorized financial transactions from compromised victim bank or brokerage accounts. These transactions were paired with a Telephone Denial of Service (TDoS) attack, in which the victim's legitimate phone line was flooded with spam-like telephone calls to prevent the banks or brokerage firms from contacting the victim to verify that the transactions were legitimate.

In December 2009, a victim in Florida filed a police report stating that $399,000 had disappeared from his online brokerage account while he was simultaneously targeted in a TDoS attack. The online withdrawals occurred in four increments, with progressively larger amounts being withdrawn each time.

Cyber criminals target not only those who trade in securities but also the exchanges in which the securities are sold. These TDoS and Distributed Denial of Service (DDoS) attacks show a desire by cyber criminals to focus their efforts on high-profile financial sector targets.

Beginning in July 2009, two U.S. stock exchanges were victims of a sustained DDoS attack. The remote attack temporarily disrupted public websites but had no impact on financial market operations. A parent company of one of the exchanges stated that it had not experienced any degradation in service on its public website or core trading and data systems, which operate on a private network.

In February 2011, criminal actors placed an online advertisement infected with malicious software onto the public website for a foreign stock exchange. The malicious advertisement appeared on the victims' computers as a pop-up, alerting the user to non-existent computer infections in an attempt to trick the users into paying for and downloading rogue "antivirus" software.

Also in February, the parent company of NASDAQ confirmed that they had been the victim of a security breach by unauthorized intruders into their Director's Desk web application, a system that was not directly linked to their trading platforms, but was instead used as an online portal for senior executives and directors to share confidential information.

These types of malicious incidents highlight not only the targeting of important financial infrastructure by cyber criminals, but also the difficulty of determining consequences and intent. For example, although it seems no real-time trading environments have been compromised in these incidents, cyber criminals could be more interested in obtaining valuable insider information than in disrupting the markets.

ATM Skimming and Point of Sale Schemes

ATM skimming is also a prevalent global cyber crime. A criminal affixes a skimmer to the outside or inside of an ATM to collect card numbers and Personal Identification Number (PIN) codes. The criminal then either sells the stolen data over the Internet or makes fake cards to withdraw money from the compromised accounts.

The technology of the skimmer devices continues to improve. This technique is also being used to steal credit and debit card information from customers at gas station pumps. Bluetooth-enabled wireless skimmers were found at a string of gas stations in the Denver area attached to the inside of the gas pump. The wireless capabilities of the skimmers allowed the criminal to download the information from the skimmers instantly, as long as they were in range of the wireless network.

Even as technology improves to protect against skimming, cyber criminals are creating devices to mimic the security features of legitimate ATM hardware. For example, ATM vendors have created new anti-skimming tools that include a backlit green or blue plastic casing around the card slot to prevent skimmers from being attached. In Ireland in early 2011, cyber criminals attached several skimmers that appeared identical to the new security devices.

Point of sale (POS) terminals, which are primarily used to conduct the daily sale operations in restaurants, retail stores, and places of business, have been a primary target for cyber criminals engaging in credit card fraud and have resulted in the compromise of millions of credit and debit cards the U.S. For example, in March 2008, three men were charged with hacking into several "smart" cash registers belonging to a U.S. restaurant chain. The criminals installed "sniffer" programs that were used to steal payment data as the information was being sent from the POS terminals in the restaurant to the chain's corporate office. The stolen data resulted in more than $600,000 in losses.

Mobile Banking Exploitation

As more mobile devices have been introduced into personal, business, or government networks, they have been increasingly targeted for stealing PII. The spread of mobile banking provide additional opportunities for cyber crime. Cyber criminals have successfully demonstrated man-in-the-middle attacks against mobile phones using a variation of ZeuS malware. The malware is installed on the phone through a link imbedded in a malicious text message, and then the user is instructed to enter their complete mobile information. Because financial institutions sometimes use text messaging to verify that online transactions are initiated by a legitimate user, the infected mobile phones forward messages to the criminal, thwarting the bank's two-factor authentication.

Cyber criminals are also taking advantage of the Twitter iPhone application by sending malicious "tweets" with links to a website containing a new banking Trojan. Once installed, the Trojan disables Windows Task Manager and notifications from Windows Security Center to avoid detection. When the victim opens their online banking account or makes a credit card purchase, PII is sent to the criminal in an encrypted file.

Insider Access

The high level of trust and confidence in U.S. financial markets is based on their long-standing reliability in protecting and ensuring the integrity of their systems. Unfortunately, individuals with direct access to core processing centers may be in a position to steal intellectual property, insider information, or data that can damage the reputation of the company. An individual could leverage this information to affect stock prices or to provide other companies with a competitive advantage.

In 2010, the FBI investigated two high profile cases involving the theft or attempted theft of source code for high-frequency trading programs. The theft of these programs could cost the victim company millions of dollars in losses, allow a competitor to predict a company's actions, or give a competitor the opportunity to profit using the victim companies' strategies.

Supply Chain Infiltration

The production, packaging, and distribution of counterfeit software or hardware used by financial institutions or critical financial networks by cyber criminals could result in the compromise of proprietary data, system disruption, or complete system failure. Gaining physical and technical access to financial institutions could be accomplished by compromising trusted suppliers of technical, computer, and security equipment, software, and hardware.

Financial firms have become regular targets of supply chain attacks. For example, ATMs have been delivered with malware installed on the systems, fake endpoints on the ATM networks have been created, and individuals have posed as ATM maintenance workers. Additionally, vendors who supply services to the banking and finance sector are constant targets of cyber criminals, including those who provide services like security, authentication, and online banking platforms.

Telecommunication Network Disruption

Financial networks are highly dependent on the availability of telecommunication infrastructure. Although cyber criminals may not be able to directly target the core processing centers that support the critical financial markets, they may target the telecommunication networks to directly impact the functionality of key financial players.

In market trading, infrastructure is crucial to the success of firms that specialize in high-frequency trading as milliseconds of saved time during data processing and transmission can impact profits. As a result, many firms co-locate and buy space near the main processing center of the major exchanges. The close proximity of these networks adds a shared reliance on telecommunication infrastructures, which could be significant if there is a disruption to the infrastructure.

Financial Estimates of Damages

Cyber criminals are forming private, trusted, and organized groups to conduct cyber crime. The adoption of specialized skill sets and professionalized business practices by these criminals is steadily increasing the complexity of cyber crime by providing actors of all technical abilities with the necessary tools and resources to conduct cyber crime. Not only are criminals advancing their abilities to attack a system remotely, but they are becoming adept at tricking victims into compromising their own systems. Once a system is compromised, cyber criminals will use their accesses to obtain PII, which includes online banking/brokerage account credentials and credit card numbers of individuals and businesses that can be used for financial gain. As cyber crime groups increasingly recruit experienced actors and pool resources and knowledge, they advance their ability to be successful in crimes against more profitable targets and will learn the skills necessary to evade the security industry and law enforcement.

The potential economic consequences are severe. The sting of a cyber crime is not felt equally across the board. A small company may not be able to survive even one significant cyber attack. On the other hand, companies may not even realize that they have been victimized by cyber criminals until weeks, maybe even months later. Victim companies range in size and industry. Often, businesses are unable to recoup their losses, and it may be impossible to estimate their damage. Many companies prefer not to disclose that their systems have been compromised, so they absorb the loss, making it impossible to accurately calculate damages.

As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates. Over the past five years, estimates of the costs of cyber crime to the U.S. economy have ranged from millions to hundreds of billions. A 2010 study conducted by the Ponemon Institute estimated that the median annual cost of cyber crime to an individual victim organization ranges from 1 million to 52 million dollars.

Addressing the Threat

Although our cyber adversaries' capabilities are at an all-time high, combating this challenge is a top priority of the FBI and the entire government. Thanks to Congress and the administration, we are devoting significant resources to this threat. Our partnerships within industry, academia, and across all of government have also led to a dramatic improvement in our ability to combat this threat. Additionally, the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC) seeks to address this threat by increasing the security of online transactions through the development of more trustworthy digital credentials which will help to reduce account takeovers and raise overall consumer safety levels.

The FBI's statutory authority, expertise, and ability to combine resources across multiple programs make it uniquely situated to investigate, collect, and disseminate intelligence about and counter cyber threats from criminals, nation-states, and terrorists.

The FBI plays a substantial role in the Comprehensive National Cybersecurity Initiative (CNCI), the interagency strategy to protect our digital infrastructure as a national security priority. Through the CNCI, we and our partners collaborate to collect intelligence, gain visibility on our adversaries, and facilitate dissemination of critical information to decision makers.

The FBI has cyber squads in each of our 56 field offices, with more than 1,000 advanced cyber-trained FBI agents, analysts, and forensic examiners. We have increased the capabilities of our employees by selectively seeking candidates with technical skills and enhancing our cyber training.

In addition, the FBI's presence in Legal Attachés in 61 cities around the world assists in the critical exchange of case related information and the situational awareness of current threats, helping to combat the global scale and scope of cyber breaches. The FBI is also changing to adapt to the ever-evolving technology and schemes used by cyber criminals. Intelligence now drives operations in the FBI. The Bureau is working in new ways with long-standing and new partners to address the cybersecurity threat.

In addition, as part of the FBI's overall transformation to an intelligence-driven organization, the Cyber Division has implemented Threat Focus Cells, which bring together subject matter experts from various agencies to collaborate and address specific identified cyber threats.

Partnerships

However, one agency cannot combat the threat alone. Through the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), we coordinate our efforts with 20 law enforcement and Intelligence Community (IC) entities, including the Central Intelligence Agency (CIA), Department of Defense (DoD), Department of Homeland Security (DHS), and National Security Agency (NSA). The FBI also has embedded cyber staff in other IC agencies through joint duty and detailee assignments.

We have also enhanced our partnership with DHS, forming joint FBI-DHS teams to conduct voluntary assessments for critical infrastructure owners and operators who are concerned about the network security of their industrial control systems (ICSs). DHS has provided more than 30 FBI agents and intelligence analysts with specialized training in these systems.

To support small businesses, we have also partnered with the National Institute of Standards and Technology (NIST) and the Small Business Administration (SBA) since 2002 to sponsor computer security workshops and provide online support for small businesses through the InfraGard program. These workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems.

In addition, because of the frequent foreign nexus to cyber threats, we work closely with our international law enforcement and intelligence partners.

We currently have FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations: Estonia, the Netherlands, Romania, Ukraine, and Colombia. These cyber personnel have identified cyber organized crime groups targeting U.S. interests and supported other FBI investigations. We have trained foreign law enforcement officers from more than 40 nations in cyber investigative techniques over the past two years.

We have engaged our international allies, including Australia, New Zealand, Canada, and the United Kingdom, in strategic discussions that have resulted in increased operational coordination on intrusion activity and cyber threat investigations.

The FBI has worked with a number of regulatory agencies to determine the scope of the financial cyber crime threat, develop mitigation strategies, and provide Public Service Announcements where appropriate, to include the U.S. Department of Treasury – Financial Crimes Enforcement Network (FinCEN), Financial Services Information Sharing and Analysis Center (FS-ISAC), the Securities and Exchange Commission (SEC), the Office of Comptroller of Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board, and the Federal Reserve Bank.

In addition, the FBI partners with criminal investigators from the Internal Revenue Service (IRS), the U.S. Secret Service (USSS), U.S. Immigration and Customs Enforcement (ICE), the Department of State's Bureau of Diplomatic Security Service (DSS), and the U.S. Postal Inspection Service to further investigations.

Additionally, the FBI works with a number of industry governing entities such as NACHA – the Electronic Payments Association and the Financial Industry Regulatory Authority (FINRA) to understand and investigate cyber crime problems affecting a particular industry segment.

Information Sharing

The FBI has developed strong relationships with private industry and the public. InfraGard is a premier example of the success of public-private partnerships. Under this initiative, state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry work with us through our field offices to ward off attacks against critical infrastructure. Over the past 15 years, we have seen this initiative grow from a single chapter in the Cleveland field office to more than 86 chapters in 56 field offices with 42,000 members.

The exchange of knowledge, experience, and resources is invaluable and contributes immeasurably to our homeland security. Notably, DHS has recognized the value of the program and recently partnered with the InfraGard program to provide joint training and

conferences during this fiscal year.

With outside funding from DHS, the newly formed Joint Critical Infrastructure Partnership will host five regional conferences this year along with representation at a number of smaller venues. The focus of the program is to further expand the information flow to the private sector by not only reaching out to the current InfraGard membership but also reaching beyond current members to local critical infrastructure and key resource owners and operators. The goal is to raise awareness of risks to the nation's infrastructure and to better educate the public about infrastructure security initiatives. This partnership is a platform which will enhance the risk management capabilities of local communities by providing security information, education, training, and other solutions to protect, prevent, and respond to terrorist attacks, natural disasters, and other hazards, such as the crisis currently facing Japan. Ensuring that a country's infrastructure is protected and resilient is key to national security.

Experience has shown that establishing rapport with the members translates into a greater flow of information within applicable legal boundaries, and this rapport can only be developed when FBI personnel have the necessary time and resources to focus on the program. This conduit for information results in the improved protection of the infrastructure of the U.S.

In the last few years, there has been a push to partner FBI intelligence analysts with private sector experts. This is an opportunity for the intelligence analysts to learn more about the industries they are supporting. They can then better identify the needs of those industries as well as FBI information gaps. Additionally, they develop points-of-contact within those industries who can evaluate and assist in timely analysis, and the analysts mature into subject matter experts.

Other successful cyber partnerships include the Internet Crime Complaint Center (IC3) and the National Cyber-Forensics and Training Alliance (NCFTA). Established in 2000, the IC3 is a partnership between the FBI and the National White Collar Crime Center that serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. Since it began, the IC3 has processed more than 2 million complaints. Complaints are referred to local, state, federal and international law enforcement and are also the basis for intelligence products and public service announcements. The FBI's IC3 unit works with the private sector, individually and through working groups, professional organizations, and InfraGard, to cultivate relationships, inform industry of threats, identify intelligence, and develop investigative information to enhance or initiate investigations by law enforcement.

The NCFTA is a private nonprofit organization, composed of representatives of industry and academia, which partners with the FBI. The NCFTA, in cooperation with the FBI, develops responses to evolving threats to the nation's critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training. The NCFTA work products can be provided to industry, academia, law enforcement, and the public as

appropriate.

The FBI and DHS also partners with the U.S. private sector on the Domestic Security Alliance Council (DSAC). This strategic collaboration enhances communications and promotes effective exchanges of information in order to prevent, detect, and investigate criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

The DSAC is in a unique position to speak on behalf of the private sector because the DSAC members are the highest ranking security executives of the member companies, who directly report to the leaders of their organizations.

Threat Mitigation

The FBI has been able to mitigate a number of fraud matters by sharing identified threat data amongst financial sector partners. The FBI participates in other activities with the private sector, like the FS-ISAC. A good example of this cooperation is the FBI's identification of a bank fraud trend in which U.S. banks were unaware that they were being defrauded by businesses in another country. As a result of FBI intelligence analysis, a joint FBI/FS-ISAC document was drafted and sent to the FS-ISAC's membership, alerting them to these crimes and providing recommendations on how to protect themselves from falling victim to the same scheme.

Another recent success was the combined efforts of the FBI, DOJ, and industry subject matter experts to takedown the "Coreflood" botnet. This botnet infected user computers and transferred banking credentials and other sensitive information to the botnet's command-and control services. This botnet infected millions of computers and the criminals used the stolen information to steal millions of dollars from unsuspecting consumers. In this instance, government and private industry worked together to provide an innovative response to a cyber threat. Not only was the Coreflood botnet shut down through a temporary restraining order, the government was authorized to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running. This prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the U.S.

Conclusion

As the Subcommittee knows, we face significant challenges in our efforts to combat cyber crime. In the current technological environment, there are growing avenues for cyber crimes against the U.S. financial infrastructure and consumers. Modifications to business and financial institution security and risk management practices will directly affect the future of these types of crimes, and the adoption of best practices may be negated by the lack of security-conscious behavior by customers.

Malicious cyber incidents are costly and inconvenient to financial institutions and their

customers, and although most businesses take action to recover quickly, limit impact to customers, and ensure long-term operational viability, the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime.

To bolster the efforts of the FBI against these cyber criminals, we will continue to share information with government agencies and private industry consistent with applicable laws and policies. We will continue to engage in strategy discussions with other government agencies and the private sector to ensure that cyber threats are countered swiftly and efficiently. We will also continue to explore innovation methods of mitigating the threats posed by cyber crime. We look forward to working with the Subcommittee and Congress as a whole to determine a successful course forward.

Prepared Testimony and
Statement for the Record of

Brian Tillett
Chief Security Strategist
Public Sector
Symantec Corporation

Hearing on

Cybersecurity: Threats to the Financial Sector

Before the

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

September 14, 2011

2128 Rayburn House Office Building

INTRODUCTION

Chairman Capito, Ranking Member Maloney, and Members of the Subcommittee, thank you for the opportunity to appear before you today as the Committee considers cybersecurity and threats to the financial sector.

My name is Brian Tillett, and I am the Chief Security Strategist for Symantec's Public Sector group, where I am responsible for the creation, dissemination and execution of security policy for the public sector team. I have been in the security and information technology fields for 18 years, beginning with my service in the U.S. Air Force, where I was assigned to the Air Force Pentagon Communications Agency and ultimately managed the Pentagon Secure Cryptographic Telecommunications Facility. As an engineer, I have also worked for a number of technology companies. I am in my fourth year at Symantec where I spend the majority of my time with government and industry partners collaborating to understand and address real world cyber threats around the globe.

Symantec[1] is the world's information security leader with over 25 years of experience in developing Internet security technology. Today we protect more people and businesses from more online threats than anyone in the world. We maintain eleven Security Response Centers globally and utilize over 240,000 attack sensors in more than 200 countries to track malicious activity 24 hours a day, 365 days a year. Our best-in-class Global Intelligence Network allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape including emerging cyber attack trends, malicious code activity, phishing and spam. In short, if there is a class of threat on the Internet, Symantec knows about it.

At Symantec, we are committed to assuring the security, availability, and integrity of our customers' information and the protection of critical infrastructure is a top priority for us. We believe that critical infrastructure protection is an essential element of a resilient and secure nation. From water systems to computer networks, power grids to cellular phone towers, risks to critical infrastructure can result from a complex combination of threats and hazards, including terrorist attacks, accidents, and natural disasters.

Symantec welcomes the opportunity to provide comments as the Committee continues its important efforts to ensure that adequate policies and procedures are in place, both in the private sector and in the federal government, to monitor and secure critical financial systems from cyber attack. In my testimony today, I will provide the Committee with:

- our latest analysis of the threat landscape as detailed in the Symantec Internet Security Threat Report Volume XVI (ISTR XVI) and in the 2011 Norton Cybercrime Report;
- an assessment of threats to the financial sector; and
- risk mitigation measures for addressing the threat.

[1] Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

THREAT LANDSCAPE

The threats we face are constantly evolving, and it is our goal to ensure that we are thinking ten steps ahead of the attackers. Looking at the current threat landscape is not enough – we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report Volume XVI, we observed significant changes to the threat landscape in 2010.[2] The volume and sophistication of threat activity increased more than 19 percent over 2009, with Symantec identifying more than 286 million unique variations of malicious software or malware. These included threats to social networking sites and users, mobile devices, and phishing.

However, to understand the evolving threat landscape, we first need to look at who is behind the vast array of cyber attacks that we are seeing today. Attacks originate from a range of individuals and organizations, with a wide variety of motivations and intended consequences. Attackers can include hackers (both individual and organized gangs), cybercriminals (from petty operators to organized syndicates), cyber spies (industrial and nation state), and "hacktivists" (with a specific political or social agenda). Consequences can also take many forms, from stealing resources and information, to extorting money, to outright destruction of information systems.

It is also important to recognize that attackers have no boundaries when it comes to their intended victims. All organizations and individuals are potential targets. Corporate enterprises are often the object of targeted attacks not only to steal customer data and intellectual property, but also to disrupt business processes and commerce. Small businesses are often less resilient and the impacts of stolen bank accounts and business disruption can be catastrophic in a very short time frame. In addition, end-users or consumers are confronted with the financial and disruptive impacts of identity theft, scams, and system clean-ups, not to mention the lost productivity and frustration of restoring their accounts. Finally, governments are most often the victims of cyber sabotage, cyber espionage, and hactivism, all of which can have significant national security implications.

Over the years, we have observed an ominous change that has swept across the Internet. The threat landscape once dominated by worms and viruses developed by irresponsible hackers is now being ruled by a new breed of cybercriminals. Cybercrime has many facets and occurs in a variety of scenarios, using a variety of methods. As more people have access to technology, criminals leverage it for criminal purposes. Just last week we released our 2011 Norton Cybercrime Report where we examined online behavior in 24 countries and interviewed nearly 20,000 consumers. We calculated the cost of global cybercrime at $114 billion annually.[3] We also calculated that lost time due to recovery and impact on personal lives was an additional $274 billion worldwide. Further, we found that more than two-thirds of online adults (69 percent) have been a victim of cybercrime in their lifetime. Every second, 14 adults become a victim of cybercrime, resulting in more than one million cybercrime victims every day[4]. These numbers are astounding.

---

[2] *Symantec Internet Security Threat Report XVI, April 2011.* http://www.symantec.com/business/threatreport/index.jsp
[3] *2011 Norton Cybercrime Report.* *www.norton.com/cybercrimereport*
[4] *Id.*

With an estimated 431 million adult victims globally in the past year, and at an annual combined cost of $388 billion globally based on financial losses and time lost, cybercrime costs are significantly more than the global black market in marijuana, cocaine and heroin combined ($288 billion).[5]

It is not just our computers that we need to secure from cybercriminals. Today, a high percentage of consumers use their mobile phones to conduct nearly every aspect of their life, from basic communication to online shopping to mobile banking. Most of these phones are not secure. The Norton Cybercrime Report revealed that 10 percent of adults online have experienced cybercrime on their mobile phone. Further, we reported in the Symantec ISTR XVI that there were 42 percent more mobile vulnerabilities in 2010 compared to 2009 – a sign that cybercriminals are starting to focus their efforts on the mobile space.

Recently, there has been an up-swing in press reports regarding cyber attacks and the "advanced persistent threat" or APT. While APT is one of the most overused terms in the security industry today, it is nevertheless something to be taken seriously. APTs covertly infiltrate systems and hide and wait for opportune moments to steal information or damage systems.

The APT is not one entity; rather it is many different and independent entities, with a tremendous range of motivations for their endeavors. Some of these motivations include financial gain, exfiltration of sensitive and personal information, cyber espionage, and a new turn in the last 18 months, cyber sabotage as exemplified by the Stuxnet malware.

Another trait of the APT is to infiltrate a system, enterprise, or organization, but not immediately execute the ultimate mission. Often the APT will lie in wait, gaining intelligence, observing patterns, and use this information to glean information to further refine the ultimate attack. The APT will even go so far as to patch systems that it finds are un-patched or vulnerable to other attacks. This is done for several reasons, including to ensure that no one else within the targeted organization finds the vulnerability or path that the APT took to get into the enterprise or system; and to make sure that no other APT or other outside rogue entity can exploit the same vulnerability or path into the enterprise.

The threats we are seeing are not new, they are just newly packaged. However, while the attacks are not new, they are becoming more targeted and the monetary losses have grown exponentially.

THREATS TO THE FINANCIAL SECTOR

We have been monitoring an array of threats to the financial sector for many years, and some of the trends we have identified are associated directly with cybercrime, ATM heists, fraud, and Banking Trojans. As observed in the ISTR XVI, the financial sector was the top sector in 2010 for identities exposed in data breaches, with 23 percent—although this was a dramatic decrease from 60 percent in 2009.[6] It is forecasted that these threats will only continue to mature and increase as society becomes more dependent on using IT for financial and banking needs. Further, with the proliferation of mobile devices -- note that 35 percent of American adults now use smartphones -- mobile banking is expected to increase significantly, as well as the threats targeted at mobile users.[7]

---

[5] *Id.*
[6] *Symantec Internet Security Threat Report XVI, April 2011.* http://www.symantec.com/business/threatreport/index.jsp
[7] *Smart Phone Adoption & Usage, Pew Internet & Life Project, Aaron Smith, http://pewinternet.org/Reports/2011/Smartphones.aspx*

- ***Botnets***

A botnet is group of computers which have been compromised and brought under the control of an individual. The individual uses malware installed on the compromised computers to launch denial-of-service attacks, send spam, or perpetrate other malicious acts.[8]

One such botnet targeting the financial services industry is called "Qakbot". It is a sophisticated worm that has been spreading through network shares, removable drives, and infected web pages, and infecting computers since mid-2009. Its primary purpose is to steal online bank account information from compromised computers. The malware controllers use the stolen information to access client accounts within various financial service websites with the intent of moving currency to accounts from which they can withdraw funds. It employs a classic keylogger, (software that monitors and captures everything a user types into a computer keyboard) but it is unique in that it also steals active session authentication tokens and then piggy backs on the existing online banking sessions. It then quickly uses that information for malicious purposes.

One of the most important attributes of Qakbot is that it is not focused on the financial institutions themselves, but rather the consumer and their individual financial transaction sessions. It is aimed at infecting and exploiting as many individual consumer transactions as possible. Financial institutions are doing their due diligence with security technologies to thwart this malware from infecting their internal systems. It is the consumer and their mobile and other devices that are vulnerable to this threat.

With more and more users performing financial transactions online on a regular basis, the underground malware society is ramping up efforts to profit from this huge consumer base. Information-stealing malware continues to be prevalent; however, very few have shown the sophistication and continued evolution presented by Qakbot. Analysis of a recent version of Qakbot shows that this malware can result in significant monetary loss for infected networks. By capturing and sending session information to the malware controllers in real time, the malware authors are able to extend legitimate online sessions, gain quick and comprehensive access to end-user bank accounts, and make transfers without giving the banks much reason to believe something is amiss.

Based on the changes observed in the recent Qakbot version, we expect continued evolution of the threat, along with additional changes to the list of targeted financial institutions. We have already seen additions made that would enable the malware authors to control what data the infected host sees. This same code could be used on a per user basis to manipulate the account balances that are seen when a legitimate user visits his or her banking institution's website. At present, the attackers can remove links that allow users to terminate online sessions. In the future, it may be possible for the worm authors to mask the evidence of any stolen money by displaying the end user's balance information prior to malicious actions occurring.

One effective means of blocking the actions of Qakbot is forcing a second mode of authentication. Additionally, it is effective to force user authorization when online accounts are used to make transfers. Even after hijacking an unsuspecting client's session, the malware controllers would not be able to complete the "challenge handshake" in order to remove funds from the account.[9]

---

[8] *Symantec, W.32 Qakbot in Detail, June 2011.*
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf
[9] *Symantec White Paper, W.32 Qakbot in Detail, June 2011,*
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_qakbot_in_detail.pdf

- ***Banking Trojans***

Malware continues to grow at exponential rates, with Trojans now being the most common type – 66 percent of all malware.[10] Trojans infect a victim's computer to enable a cybercriminal to perform malicious functions, such as making it part of a botnet (a collection of remotely-controlled computers) or stealing confidential data like passwords and credit card information. Banking malware, specifically banking Trojans, are reaching alarming new levels of sophistication. New variations are constantly being introduced to thwart detection by antivirus software, and real-time capabilities built into the Trojans make it difficult for banks and account holders to spot fraud attempts as they occur.

Trojans today pose a clear threat to the trust in online banking that financial institutions have worked so hard to establish for their customers, let alone the extensive losses associated with fraud and potential lawsuits. For example, in 2009, a Maine- based construction firm sued its local bank after cyber thieves stole more than a half million dollars through illegal transfers from the company's online account.[11]

The most prevalent of all banking Trojans is known as Zeus. Hundreds of criminal groups are operating Zeus-fueled botnets or Zbot botnets. The number of infected PCs is estimated at 3.6 million in the U.S., or one percent of all PCs in the country.[12] Zeus has been stealing data and circulating since 2006, capturing infected users' banking logon credentials and sending them back to a command-and-control hub. Zeus is propagated through scams such as spam messages purportedly from well known telecommunications and software companies, social networking sites, and government agencies.

Zeus infects PCs, waits for their users to log on to a list of targeted banks and financial institutions, steals their credentials and sends them to a remote server in real-time. In addition, it may inject code into the web pages shown by a user's browser, so that its own content is displayed together with (or instead of) the genuine pages from the bank's Web server. In this way it is able to ask the user to divulge additional personal information, such as payment card number and PIN, one-time passwords, and more.

To evade detection and removal, Zeus uses rootkit techniques. The Zeus kit is a binary generator. Each use creates a new binary file, and these files are different from each other — making them notoriously difficult for antivirus or security software to detect. To date, very few variants have had effective antivirus signatures against them, and each use of the kit usually makes existing signatures ineffective.

Using Zeus or other banking Trojans, cybercriminals can bypass many of today's standard security mechanisms. That is why a layered security defense is critical: no one security component is fail-proof against every possible threat. It takes a multilayer strategy to defend against sophisticated fraud attempts. By layering technology such as two-factor authentication and fraud detection, financial services companies can better protect themselves and their customers.

- ***ATM Heists***

Over the past two years, cyber ATM heists have accounted for nearly $30 million in fraudulent transactions. Recently, an international cybercrime gang stole $13 million from a Florida-based bank by

---

[10] *Symantec White Paper, Banking Trojans: Understanding Their Impact and How they Impact Your Institution, http://www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_info_risk_comp&pvid=fds_1*
[11] *Id.*
[12] *Id.*

cashing out stolen pre-paid debit cards.[13] The attackers were able to breach the institution's network, targeted pre-paid debit cards, and distribute the cloned prepaid cards globally.

In 2009, another similarly coordinated attack resulted in the heist of $9 million in cash, after a hacker penetrated a server at a payment processor. About a month later, the processor announced that they'd been hacked, and personal information on approximately 1.5 million payroll-card and gift-card customers had been stolen.[14]

Another scheme in 2007 targeted a payment card company. In just two days, four payment cards were hit with more than 9,000 actual and attempted withdrawals from ATM machines around the world, resulting in losses of $5 million. A similar technique was employed against a major financial institution last year, after a processing server that handled withdrawals from the bank's ATMs at convenience stores was breached. In that case, cashers converged on a major northeast city and withdrew at least $2 million from the bank's accounts and then sent most of it out of the country.[15]

- ***Mobile Devices, Payment, and Banking Applications***

With the increased use of mobile phones for banking comes increased risks. As more users download and install third-party applications for mobile devices, the opportunity for installing malicious applications is also increasing. Most malicious code is now designed to generate revenue. Hence, there will likely be more threats created for these devices as people increasingly use them for sensitive transactions such as online shopping and banking. Trojans that steal data from mobile devices and phishing attacks are some of the first of these threats to arrive.

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals globally, there was a 42 percent increase in the number of reported new mobile operating system vulnerabilities from 2009 to 2010.[16] Currently, the majority of malicious code for mobile devices is in the form of Trojans that pose as legitimate applications. These applications are uploaded to mobile application marketplaces where users download and install them. In some cases, attackers may take a popular legitimate application and add additional code to it, as happened in the case of the Pjapps Trojan. Indications from the ISTR XVI are such that not only are the operating systems of the mobile devices prime targets for threats, malware, and exploited vulnerabilities, but the applications (or Apps) that are used on these mobile devices are increasingly growing as threat vectors.

The potential for fake and/or rogue applications that are designed to look, feel, and act like a trusted mobile banking application are an increasing threat and propagation method for malware and illicit activity. Often, the propagation/enticement method includes a "free" version of a popular application that an individual would normally have to pay for. The unknowing consumer opts to download the "free" version of the application, which could be a financial management/banking application, or any type of application, and once the application is downloaded to the mobile device, the malware begins to execute without the user's knowledge.

---

[13] *Coordinated ATM Heists Net Hackers $13M, Brian Krebs, Krebs on Security Blog, August 26, 2011*
[14] *Global ATM Caper Nets Hackers $9 Million in One Day, Kevin Poulsen, Wired, 2/4/09*
[15] *Id.*
[16] *Id.*

The safest and most secure mobile banking application transactions utilize technologies including but not limited to: encryption of information during transmission; encryption of any persistent information stored on the mobile device; authentication and tracking of the device based on constant attributes of the mobile device associated with that user account; and lastly and most significant, two-factor authentication including a persistent PIN and a onetime use password which is initiated once per transaction. The onetime use password via two-factor authentication is a significant security measure that allows only one person to be authenticated to a financial transaction application for a singular session. Once that session is completed, another two-factor authentication takes place producing another singular session that can be tracked and logged to provide an accountability system of checks and balances.

FINANCIAL SERVICES LEADS IN SECURITY

The financial services sector has been a leader in taking both voluntary and required measures toward the goal of cybersecurity protection for their customers, commercial clients and their own franchises. Industry professionals are increasingly focused on safeguards, investing tens of billions of dollars in data protection as they recognize the criticality of confidentiality, reliability and confidence to their success in the marketplace as well as national security. This market-based discipline is enforced through an increasingly informed consumer base, and by a very active commercial clientele that often specifies security standards and negotiates for audit and notification rights.

To strengthen public confidence and to ensure consistency across a wide variety of institutions, self-regulatory organizations and government agencies codify and enforce a comprehensive system of requirements. Many of these represent the distillation of best practices previously developed on a voluntary, collaborative basis by the industry and codified into law by this Committee. These include the provisions of Gramm-Leach-Bliley, the Financial Services Modernization Act of 1999, which fostered the promulgation of Regulation P by the Federal Financial Institutions Examinations Council (FFIEC) and Regulation S-P by the Securities and Exchange Commission (SEC). These oversight mechanisms of data security are unique to the financial services industry.

This Committee, and the financial services industry generally, has been ahead of the curve on cybersecurity, recognizing the importance of these issues long before they were common in daily headlines. Thus, the need for action is not so much an issue of additional legislation or regulation, but rather an issue of responding to evolving threats by implementing mitigation and protection measures.

MITIGATING RISKS

There are a number of steps that industry can take to lessen the impact or prevent future attacks. We recommend the following measures be implemented to better protect critical systems from cyber attack:

- **Develop and enforce IT policies** and automate compliance processes. By prioritizing risks and defining policies that span across all locations, organizations can enforce policies through built-in automation and workflow and not only identify threats but remediate incidents as they occur or anticipate them before they happen.
- **Protect information** proactively by taking an information-centric approach. Taking a content-aware approach to protecting information is key in knowing who owns the information, where sensitive information resides, who has access, and how to protect it as it is coming in or leaving

your organization. Utilize encryption to secure sensitive information and prohibit access by unauthorized individuals.

- **Authenticate identities** by leveraging solutions that allow businesses to ensure only authorized personnel have access to systems. Authentication also enables organizations to protect public facing assets by ensuring the true identity of a device, system, or application is authentic. This prevents individuals from accidentally disclosing credentials to an attack site and from attaching unauthorized devices to the infrastructure.
- **Manage systems** by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on system status.
- **Protect the infrastructure** by securing endpoints, messaging and Web environments. In addition, defending critical internal servers and implementing the ability to back up and recover data should be priorities. Organizations also need the visibility and security intelligence to respond to threats rapidly.
- **Ensure 24x7 availability.** Organizations should implement testing methods that are non-disruptive and they can reduce complexity by automating failover. Virtual environments should be treated the same as a physical environment, showing the need for organizations to adopt more cross-platform and cross-environment tools, or standardize on fewer platforms.
- **Develop an information management strategy** that includes an information retention plan and policies. Organizations need to stop using backup for archiving, implement de-duplication everywhere to free up resources, use a full-featured archive system and deploy data loss prevention technologies.

However, while technological improvements are necessary, they must be paired with increased education and awareness. People, processes, organization and technology must all be addressed to mitigate cyber threats. We see the need for improved education efforts across the spectrum of learning institutions from the classroom and colleges, to corporate management and professional education.

We also need to embrace new and evolving security technologies, rather than looking to simply refine traditional security technologies around the changing threat landscape. An example of this is how to best address the APT. The design of the APT is to gain massive amounts of intelligence about a target before launching an attack. The financial organization, enterprise, or entity needs to understand and use this intelligence about how they normally do business and secure this from an offensive perspective. Once the financial organization has a blueprint of their normal business processes and hardens these processes, anything outside of the norm can be detected as an anomaly, and systems can be protected. This is the primary method for defending against APT types of malicious activity at the core of infrastructure protection.

Successful mitigation of cyber threats also requires increased coordination and communication among industry and between government and industry. Currently, there are a number of organizations in place to facilitate information sharing, including Information Sharing and Analysis Centers (ISACs) and the National Cyber-Forensics and Training Alliance (NCFTA).

- ***ISACs***

ISACs were established in the late 1990s as a result of the recognition by industry and government that more needed to be done to address critical infrastructure security. Today, the majority of ISACs are operated by the private sector, and facilitate information sharing and comprehensive sector analysis on both physical and cyber events across their industry members, and with other ISACs through the National Council of ISACs. In addition, a number of the ISACs have established partnerships with various government agencies whereby information is shared, and incidents are jointly worked by government and industry. Services provided by ISACs include risk mitigation, incident response, and alert and information sharing. There are ISACs that represent IT (of which we are a member), Financial Services, Communications, Energy, and several other critical sectors.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was established in 2002, and today reaches more than 20,000 industry partners daily. The FS-ISAC is considered a successful model for other ISACs, with its broad range of 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, and financial advisory services. In addition to supporting the needs of the financial services sector, it works closely with other ISACs and government partners to protect critical financial services and facilitate strong information sharing.

- ***NCFTA***

Established as a non-profit corporation to address cybercrime, the NCFTA is a non-profit corporation that comprises a large network of experts from the public and private sectors. Functioning as a conduit between private industry and law enforcement, the NCFTA's core mission is to work with law enforcement to identify criminals or criminal groups responsible for cyber-based threats, and to provide law enforcement with actionable intelligence to mitigate threats.

The NCFTA has pursued a number of successful activities to neutralize cybercrime, including proactive law enforcement engagement (domestically and internationally), and implementation of interim technology solutions (i.e., null-routing of botnet traffic or similar interdiction action via Top Level Domains or ICANN).

The NCFTA regularly supports interaction into threat-specific initiatives to promote better intelligence sharing between the NCFTA and law enforcement. After a major cyber crime trend is identified, members of the NCFTA develop a tailored program whereby the NCFTA manages the collection and sharing of information with industry partners, appropriate law enforcement, and other cross-sector experts. As a result of these initiatives, hundreds of criminal (and some civil) investigations have been launched, with successful prosecutions of more than 300 cyber criminals worldwide. In addition, in the past three years alone, the NCFTA has developed more than 400 cyber threat intelligence reports to assist partners in mitigating the threats of cybercrime.

Over the years progress has been made to advance information sharing among critical infrastructure sector partners and the government. Organizations such as the NCFTA and FS-ISAC have done a commendable job of creating mechanisms to share intelligence among industry and between industry and government. In order to successfully mitigate against these threats however, information must be shared in a timely and actionable manner. In addition, there are still significant impediments to

government sharing information with industry, including classification designations, legal restrictions, and competitive advantage concerns.

CONCLUSION

I applaud the Committee's commitment to this critical topic and its leadership on data security issues for more than a decade. As the threats we face today continue to escalate in both sophistication and volume, we must continue to bolster cybersecurity, improve information sharing mechanisms, and increase awareness and education. Symantec looks forward to working with the Committee and our public and private sector partners to address these important issues.

○