AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE STATE OF SMALL BUSINESS SECURITY IN A CYBER ECONOMY

HEARING

BEFORE THE

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

OF THE

COMMITTEE ON SMALL BUSINESS
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

WASHINGTON, DC, MARCH 16, 2006

Serial No. 109–44

Printed for the use of the Committee on Small Business

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

U.S. GOVERNMENT PRINTING OFFICE

27–809 PDF WASHINGTON : 2006

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

COMMITTEE ON SMALL BUSINESS

DONALD A. MANZULLO, Illinois, *Chairman*

ROSCOE BARTLETT, Maryland, *Vice Chairman*
SUE KELLY, New York
STEVE CHABOT, Ohio
SAM GRAVES, Missouri
TODD AKIN, Missouri
BILL SHUSTER, Pennsylvania
MARILYN MUSGRAVE, Colorado
JEB BRADLEY, New Hampshire
STEVE KING, Iowa
THADDEUS McCOTTER, Michigan
RIC KELLER, Florida
TED POE, Texas
MICHAEL SODREL, Indiana
JEFF FORTENBERRY, Nebraska
MICHAEL FITZPATRICK, Pennsylvania
LYNN WESTMORELAND, Georgia
LOUIE GOHMERT, Texas

NYDIA VELÁZQUEZ, New York
JUANITA MILLENDER-McDONALD, California
TOM UDALL, New Mexico
DANIEL LIPINSKI, Illinois
ENI FALEOMAVAEGA, American Samoa
DONNA CHRISTENSEN, Virgin Islands
DANNY DAVIS, Illinois
ED CASE, Hawaii
MADELEINE BORDALLO, Guam
RAÚL GRIJALVA, Arizona
MICHAEL MICHAUD, Maine
LINDA SÁNCHEZ, California
JOHN BARROW, Georgia
MELISSA BEAN, Illinois
GWEN MOORE, Wisconsin

J. MATTHEW SZYMANSKI, *Chief of Staff*
PHIL ESKELAND, *Deputy Chief of Staff/Policy Director*
MICHAEL DAY, *Minority Staff Director*

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

W. TODD AKIN, Missouri *Chairman*
MICHAEL SODREL, Indiana
LYNN WESTMORELAND, Georgia
LOUIE GOHMERT, Texas
SUE KELLY, New York
STEVE KING, Iowa
TED POE, Texas

MADELEINE BORDALLO, Guam
ENI F. H. FALEOMAVAEGA, American Samoa
DONNA CHRISTENSEN, Virgin Islands
ED CASE, Hawaii
LINDA SÁNCHEZ, California
GWEN MOORE, Wisconsin

CHRISTOPHER SZYMANSKI, *Professional Staff*

CONTENTS

WITNESSES

	Page
Furlani, Ms. Cita M., Acting Director, Information Technology Laboratory, National Institute of Standards and Technology	3
Parnes, Ms. Lydia, Director of Bureau of Consumer Protection, Federal Trade Commission	5
Johnson, Mr. Larry D., Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service	7
Martinez, Mr. Steven M., Deputy Assistant Director Cyber Division, Federal Bureau of Investigations	9
Schwartz, Mr. Ari, Deputy Director, Center for Democracy and Technology	17
Salem, Mr. Enrique, Senior Vice President, Security Products & Solutions, Symantec Corporation	18
Kaliski, Dr. Burton S., Jr., Vice President of Research, RSA Security, Chief Scientist, RSA Laboratories	20
Cochetti, Mr. Roger, Group Director—U.S. Public Policy, Computing Technology Industry Association	22
Schmidt, Mr. Howard, President & CEO, R & H Security Consulting, LLC.	24

APPENDIX

Opening statements:	
Akin, Hon. W. Todd	34
Prepared statements:	
Furlani, Ms. Cita M., Acting Director, Information Technology Laboratory, National Institute of Standards and Technology	35
Parnes, Ms. Lydia, Director of Bureau of Consumer Protection, Federal Trade Commission	42
Johnson, Mr. Larry D., Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service	59
Martinez, Mr. Steven M., Deputy Assistant Director Cyber Division, Federal Bureau of Investigations	64
Schwartz, Mr. Ari, Deputy Director, Center for Democracy and Technology	68
Salem, Mr. Enrique, Senior Vice President, Security Products & Solutions, Symantec Corporation	75
Kaliski, Dr. Burton S., Jr., Vice President of Research, RSA Security, Chief Scientist, RSA Laboratories	80
Cochetti, Mr. Roger, Group Director—U.S. Public Policy, Computing Technology Industry Association	92
Schmidt, Mr. Howard, President & CEO, R & H Security Consulting, LLC.	103
Additional Material:	
National Small Business Association 2006 Malware Survey	116

THE STATE OF SMALL BUSINESS SECURITY IN A CYBER ECONOMY

THURSDAY, MARCH 16, 2006

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT
COMMITTEE ON SMALL BUSINESS
Washington, DC

The Subcommittee met, pursuant to call, at 2:00 p.m. in Room 2360 Rayburn House Office Building, Hon. W. Todd Akin [Chairman of the Subcommittee] presiding.

Present: Representatives Akin, Kelly, Bordallo.

Chairman AKIN. The hearing will come to order. Good afternoon and welcome everybody to today's hearing, "The State of Small Business Security in a Cyber Economy." I want to especially thank those witnesses who have traveled long distances to participate at this important hearing.

Today this Subcommittee seeks to better understand the impact small business cyber security has on the well-being of the economy. This Subcommittee also seeks to determine the types of threats that small businesses encounter on a daily basis. According to the Small Business Technology Institute Report released in July 2005:

"If small businesses are not made fully aware of the economic impact of information security incidents, they will continue to underinvest in information security protection, and their exposure will continue to increase as their infrastructures become more complex. This increasing individual exposure, when aggregated across the many millions of small businesses in the U.S., supporting more than half of the Nation's GDP, represents an extremely high and worsening point of exposure for the U.S. economy as a whole."

Businesses do not have to sell their products online to be at risk of a security breech. They are exposed simply by being connected to the internet. The Government and large firms have dedicated information technology professionals who protect their electronic infrastructure.

Small businesses seldom have either dedicated IT professionals or the resources necessary to provide adequate levels of protection. I look forward to hearing the testimony of your witnesses to learn more of what we can do to protect small business from cyber security threats. I now yield to the gentlelady from Guam, Madame Bordallo.

[Chairman Akin's opening statement may be found in the appendix.]

Ms. BORDALLO. Thank you very much, Mr. Chairman Before I begin my opening remarks, I would like to recognize a very young witness in our audience today and that is Mr. Andrew Cochetti. He is here on an assignment with his social studies class. Welcome, Andrew. He is the son of Roger.

Internet and telecommunication technologies have a profound impact on our daily lives. They have changed how we communicate with friends and family and how we interact with our Government.

America's 23 million small businesses are some of the savviest users of telecommunication technology using the internet to access new markets to grow and to diversify. In fact, American small businesses have a strong record of being the driving forces behind further technological innovation and the development of innovative business models that we now take for granted.

Along with being connected comes being exposed to new threats. The risks associated with turning more of our lives and business into digital i's and o's and burst of light over fiber optic cables are significant and require vigilant management. A single individual can design computer viruses that can be spread across continents in milliseconds.

Identity theft compromises credit records, businesses and, sadly, lives. Destructive computer viruses and other malicious Internet activities pose severe problems for small business owners that are not prepared to mitigate this kind of a risk. This exposure can even result in thousands of hard-earned revenues being lost.

An FBI-conducted survey of computer related crimes including viruses, spyware, and theft revealed that a total of nearly $70 billion in 2005 alone was lost with companies incurring an average of $24,000 in losses. Losses like this are make or break for some businesses, and sadly some small companies and computer users fail to recognize the benefit of cyber risk mitigation as an investment until it is too late.

The Federal Trade Commission, the FBI, the Secret Service, and the National Institute of Standards and Technology have all embarked on efforts to offer federal programs designed to educate the public on computer security. In fact, federal cyber security spending has increased from $5.6 billion in 2004 to more than $6 billion in 2007 and is expected to hit $7 billion by 2009.

I am concerned that despite the rise in cyber attacks over the past few years and the growing impact they have had on small businesses in America, the Small Business Administration, the sole agency charged with aiding America's entrepreneurs, does not have updated internet security information readily accessible on its website.

Like all of us, small firms are exposed to cyber attacks and vulnerable to their malicious affects. Today's hearing will give us an opportunity to review whether the increases in federal investment, both human and financial resources, have had or can have an impact on small firm's ability to mitigate their cyber risk.

The testimony that we hear today I hope will both help us to better understand what role the Congress and the Federal Government can play in educating the American public and the business community to the risks that they face from cyber crimes and what recommendations Congress can act on to protect Americans and

their businesses from this growing threat. I thank you, Mr. Chairman.

Chairman AKIN. Thank you for the opening statement. Also, I would like to recognize another one of our colleagues, Sue Kelly, who also comes from a very businesslike area, New York. If you would like to make an opening statement. I understand you have a vote pending in another committee and may join us later. You are welcome to proceed.

Ms. KELLY I thank you very much. I represent the New York Hudson Valley and I have been meeting recently with a number of small businesses in the Hudson Valley and this issue of cyber security and cyber economy is very high on their list. I must add that we create the IBM computers in the Hudson Valley in the district I represent. We also have the research labs for not only Phillips Electronics but IBM. This is a highly sophisticated group of people in the Hudson Valley and yet my small businesses in that area are worried even though they have access to highly sophisticated people who are actually building some of the systems so it is extremely important that you are here today. This is an issue of extreme importance for our small businesses in this nation and I look forward to your testimony. I do have a vote in another committee. I will have to go but I intend to come back to keep listening to what you have to say. Thank you very much.

Chairman AKIN. Thank you. We have got a little bit of a challenge for the Chairman today. Aside from running a little late from too many meetings, I usually like to keep things running on time but we have got a double panel so this is a double header today. Those of you who need your cups of coffee need to be forewarned.

Our first panel, as you can see, there are four people that have joined us here. It is really a Government panel and the first witness is Cita Furlani. Did I get that pretty close, Cita? You are the Acting Director of Information Technology Laboratory from the National Institute of Standards and Technology from Gaithersburg, Maryland. Is that correct?

Ms. FURLANI. Correct.

Chairman AKIN. We have the right person. What we are going to do is take five-minute statements. I would prefer to take a five-minute statement from each of you and then open up with some questions afterwards if that is okay. I think probably some of you are pros in here. You know the little light in red means that somebody is going to throw the hammer at you. Keep it within five if we could, please.

You can submit written statements for the record if you would like. I think most of us would prefer to hear you talk to us about what you think are the most important things you can communicate in five minutes. Thank you very much. Proceed, Cita.

STATEMENT OF CITA FURLANI, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Ms. FURLANI. Thank you. I appreciate this opportunity to be here today. We recognize that small businesses play an important role in the U.S. economy. Since use of the Internet is critical in the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber environ-

ment cannot be overstated. Today I will focus my testimony on NIST's cyber security programs, the National Institute of Standards and Technology, and our programs and activities that can assist small businesses.

NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Ensuring that business-related information is secure is essential to the functioning of our economy and indeed to our democracy. Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the federal government.

Since small businesses are nearly 99 percent of all U.S. businesses, a vulnerability common to a large percentage of these organizations could indeed pose a significant threat to the Nation's economy and overall security. In the interconnected environment in which we all operate, it is vital that this important sector of our economy be aware of the risks and take appropriate steps to ensure their systems are secure.

Under the Federal Information Security Management Act (FISMA), NIST was assigned the responsibility to develop IT standards and guidelines to secure federal systems. While targeted primarily toward federal agencies, these security standards and guidelines are also used widely by other organizations including small businesses.

These documents are available on our web-based Computer Security Resource Center. I brought two or three of them today to show that they really do exist but they can be downloaded. The website provides a wide range of security materials and information and has over 20 million hits annually.

In 2002 NIST partnered with the Small Business Administration and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. We have developed a small business outreach site where small businesses may find information on local workshops.

NIST also is raising the awareness of the importance of cyber security among small manufacturers. The NIST Hollings Manufacturing Extension Partnership was created to improve the competitiveness of America's smaller manufacturers and now provides the eScan Security Assessment. This diagnostic tool was designed specifically for small businesses to determine how well their IT systems are protected against failure or intrusion.

NIST with support from the Department of Homeland Security recently developed the National Vulnerability Database that integrates all publicly available U.S. Government computer vulnerability resources and provides references to industry resources. It contains information on almost 16,000 vulnerabilities and is also available on our website.

Small business, indeed all organizations, rely on the software used on their information system. We continue to work with industry to improve the security and reliability of software. For example, we develop standards and test suites for interoperable, robust,

quality web applications and products. We conduct research to improve the quality of software including software trustworthiness.

NIST works with industry and other Government agencies in research to improve the interoperability, scalability, and performance of new Internet security systems, to expedite the development of Internet infrastructure protection technologies, and to protect the core infrastructure of the Internet.

Meeting the challenge of securing our nation's IT infrastructure demands a greater emphasis on the development of security-related metrics, models, datasets, and testbeds so that new products and best practices can be evaluated. The President's FY '07 proposed budget will support NIST's collaborations with industry and academia to develop the necessary metrics and measurement techniques to provide an assessment of overall system vulnerability.

In summary, Mr. Chairman, the IT security challenge facing small businesses is indeed great. Systems managed by small businesses are part of a large, interconnected community enable by extensive networks and increased computing power. Certainly, there is great potential for malicious activity against non-secured or poorly secured systems or for accidental unauthorized disclosure of sensitive information or breach of privacy.

We believe the programs and activities described today in this testimony demonstrate our commitment to a more effective national cyber security environment as we assist small enterprises and protecting their assets.

Detailed information can be found in my written testimony which I hope you will add to the meeting minutes.

Chairman AKIN. Without objection.

Ms. FURLANI. Thank you, Mr. Chairman, for the opportunity to present NIST's views regarding security challenges facing small businesses. I will be pleased to answer any questions.

[Ms. Furlani's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Cita.

Next is Lydia Parnes. Did I get the last name right?

Ms. PARNES. It is Parnes.

Chairman AKIN. Parnes. Excuse me. Parnes. Director of the Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. You didn't have to travel too far.

Ms. PARNES. No, I didn't. Just down the block.

Chairman AKIN. Thank you, Lydia. Same thing, five minutes, please.

Ms. PARNES. Thank you.

STATEMENT OF LYDIA PARNES, FEDERAL TRADE COMMISSION

Ms. PARNES. Mr. Chairman and members of the Subcommittee, I appreciate the opportunity to appear before you today to discuss the challenges consumers and small businesses face in protecting their computer systems, as well as the Commission's efforts to promote a culture of security among all Internet users.

The views in my written testimony are those of the Commission. My oral remarks and responses to questions represent my own views and not necessarily those of the Commission or any individual Commissioner.

For more than a decade protecting the privacy of American consumers as been a top FTC priority. The explosive growth of the Internet and the development of sophisticated computer systems have made it easier than ever for companies to gather and use information about their customers.

Small businesses once limited to consumers walking into their stores on main street now reach consumers across the globe and complete transactions entirely online. These information systems provide enormous benefits. At the same time they can have serious vulnerabilities that threaten the security of information stored in them.

Securing these systems against an ever changing array of threats is challenging, particularly for small businesses. For several years the FTC has engaged in a broad outreach campaign to educate businesses and consumers about information security and the precautions they can take to protect or minimize risks to personal information.

Last September the FTC unveiled a cyber security campaign called OnGuard Online. Our campaign is built around seven online safety tips presented in modules with information on specific topics such as phishing, spyware, and spam. Each module includes articles, videos, and engaging interactive quizzes in English and in Spanish. Numerous firms including many small businesses are now using OnGuard Online materials in their own security training programs.

The FTC created OnGuard Online with consumers in mind but it is a valuable tool for small businesses as well. In many ways computer users and small firms are like home users. They employ similar applications to participate in e-commerce, send e-mail, build spreadsheets, and create presentations. And, as in the typical household, often there is no information technology professional on site.

Unlike most consumer users, however, small businesses may maintain records on hundreds, if not thousands of consumers making their computers especially attractive to information thieves. If consumers are to have confidence in our information economy, it is essential that these records be adequately protected.

The Commission recognizes that the key to developing an effective cyber security program is flexibility. The Commission Safeguards Rule, for example, requires covered financial institutions to develop written information security plans. The rule gives each company the flexibility to develop a plan that takes into account its size and complexity, the nature and scope of its activities, and the sensitivity of the consumer information it handles.

The Commission follows a similar flexible approach to its enforcement actions under Section 5 of the FTC Act. To date we have brought 12 data security cases enforcing the FTC Act and the Safeguards Rule.

The Commission also recently issued the Disposal Rule which requires all users of credit reports to dispose of them properly and not, for example, by leaving them lying in a dumpster available to identity thieves. Like the Safeguards Rule the Disposal Rule contains a flexible standard, reasonable measures to protect against unauthorized access to the information being disposed of.

Safeguarding customer information is not just the law. It also makes good business sense. When small businesses show that they care about the security of customer's personal information, they increase their customer's confidence in the company in order to help businesses of all sizes comply with both the Safeguards and Disposal Rules the FTC has issued business education materials which are available on our website.

Providing adequate security for consumer information presents challenges for everyone in the global information based economy. The Commission recognizes that this can be particularly challenging for small businesses. The Commission is committed to continuing its work promoting security awareness and sound information practices through education, enforcement, and international cooperation.

I appreciate the opportunity to testify today and look forward to the Committee's questions. Thank you.

Chairman AKIN. Thank you, Lydia. Right on time. Next witness is Larry Johnson, Special Agent in Charge of Criminal Investigative Division, United States Secret Service, Washington, D.C. Larry, thank you.

[Ms. Parnes' testimony may be found in the appendix.]

STATEMENT OF LARRY JOHNSON, U.S. SECRET SERVICE

Mr. JOHNSON. Good afternoon, Mr. Chairman The Secret Service was established in 1865 to protect our fledgling financial infrastructure through the investigation of counterfeiting and counterfeit currency. The Secret Service has adapted its investigated methodologies to accommodate the increasingly sophisticated systems we protect.

With the passage of federal laws in 1984, the Secret Service was provided the statutory authority to investigate a wide range of financial crimes to include false identification, 18 U.S.C. 1028, access device fraud, 18 U.S.C. 1029, and computer fraud, 1030.

These three statutes encompass the core violations that constitute the technology-based identity crimes that affect small businesses every day. Over the last two decades the Secret Service has conducted more than 733,000 financial fraud and identity theft investigations involving these statutes mostly involving small businesses.

Additionally, the Secret Service and the Computer Emergency Response Team, CERT, located in Carnegie Mellon University, collaborated on a project called the Insider Threat Study which was a behavioral and technical analysis of computer intrusions by organization insiders in various critical infrastructure sectors.

The Insider Threat Study provided insight to both the activities of the insiders and the vulnerabilities which they exploited. The results of this study are available on the Secret Service public website.

In 1995 in response to the ever-increasing tide of electronic crimes, the Secret Service developed a highly effective formula for combating high-tech crime. It was the Electronic Crime Task Forces, ECTF. They are an information-sharing conduit where state, local, and federal law enforcement, private industry, and financial sector, academia work together in a collaborative crime-

fighting environment. Participation includes every major federal, state, and local law enforcement agency in the region.

In 2001 the USA PATRIOT Act authorized the Secret Service to "develop a nationwide network of electronic crime task forces based on the New York Electronic Crimes Task Force model throughout the United States for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service has since launched 15 ECTFs based upon the New York model. We also have nine electronic crimes task force working groups and 24 financial crime task forces. In 2005 the Secret Service also established the Criminal Intelligence Section. This Criminal Intelligence Section provided coordination and oversight to every significant cyber case with international ties in 2003 and 4.

During this case Secret Service agents uncovered significant vulnerabilities within the computer systems of a number of Fortune 500 companies and their smaller company counterparts without alarming the public quietly notifying each of these companies of their findings, thus preventing an estimated $53 million in losses.

Estimated exposure to the U.S. financial institutions based on this case were nearly $1 billion. The success of this undercover operation led to the establishment of numerous other online undercover operations which are currently ongoing today. The Secret Service is convinced that building trusted partnerships with the private sector, and specifically small business in an effort to educate the public on how they can reduce the threats of data breaches and improve their system security is the model for combating electronic crimes in the information age.

Though a large percentage of the private sector breaches to which the Secret Service provides investigative assistance and support are large data brokers, corporations or financial institutions, we do not differentiate based upon the size of the victim or the amount of potential loss. We are equally concerned with compromises being experienced by small companies or independent service organizations or ISOs, and will respond with the appropriately trained personnel when notified of a suspected compromise. This is why we believe so strongly in a proactive educational platform as a preventative measure. Bottom line, if you are victimized, we will respond.

Through the use of company best practices you can reduce the risk of Internet crime. Some actions we recommend to small and large businesses alike include establishing internal policies and communicate them to your customers, provide a method for customers to confirm the authenticity of their e-mails, employ stronger authentication methods at websites using information other than Social Security numbers. If Social Security numbers aren't solicited on websites, this information will not be at risk. Also, monitor the Internet for phishing websites that spoof your company's legitimate sites.

Chairman AKIN. Larry, I need to stop you. You are way over here and we have got votes going on right now so I am going to try and

quickly slip you in, Steve, if we could. Then I think I am going to let Ms. Bordallo ask some questions. I am going to be gone close to half an hour voting and we will resume following that.

[Mr. Johnson's testimony may be found in the appendix.]

STATEMENT OF STEVEN MARTINEZ, FEDERAL BUREAU OF INVESTIGATION

Mr. MARTINEZ. Thank you. Good afternoon, Chairman Akin, Ranking Member Bordallo, and members of the Committee. I want to thank you for this opportunity to testify before you today about Small Business Cyber-Security Issues.

As retail business moves to the world of e-commerce, cyber crime will follow. In 2000 e-commerce accounted for 1 percent of all retail sales. Today it accounts for 2.4 percent of all sales. this upward trend will undoubtedly continue. Adding to this the revenue generated by non-retail Internet businesses, such as media and entertainment, e-commerce will soon dominate all commercial activity worldwide. The FBI is committed to investigating threats at all levels against this major force in our economy.

Small business forms a vital link in the overall security of the Internet. First, small business accounts for a significant portion of the retail business occurring on the Internet. Many online businesses and e-retailers are small businesses, many small businesses are customers of online businesses, and still other small businesses support the IT and Internet operations of large businesses and the government. Second, the integrity of Internet-connected small business systems has an impact on security of the Internet as a whole.

The FBI has recognized that the best way to combat the growing threat of cyber crime is to form a partnership with businesses and industries that rely on the Internet for their success. By teaming up with the private sector the FBI is able to find out what issues affect business and what problems are causing the most harm. This has allowed us to focus our efforts on the major problems affecting the Internet.

Further, through our outreach and information-sharing initiatives we are able to share our experiences with the business community so that they can better protect and defend themselves against new and evolving cyber threats. The education of small businesses about the scope and nature of cyber threats is an important first step in protecting those businesses.

The FBI has two initiatives focused on building a partnership with business: The National Cyber-Forensics and Training Alliance (NCFTA) and InfraGard. The NCFTA is a first-of-its-kind public-private alliance located in Pittsburgh, PA. At the NCFTA members of law enforcement work side-by-side with representatives from business on addressing the latest and most significant cyber threats. Through this collaboration the FBI has been able to identify and prosecute some of the most serious cyber criminals including those who distribute computer viruses, operate large networks of compromised computers (known as botnets), and perpetrate fraud schemes such as phishing scams. The NCFTA is strategically located near Carnegie Mellon University's Computer Emergency and Response Team/ Coordination Center (CERT/CC) and is also

within driving distance of the FBI's Internet Crime Complaint Center (1C3).

As an example on how we address cyber complaints, the NCFTA was recently contacted by a small bank in New Jersey. The bank was the victim of a phishing attack. In this type of attack the criminal creates a fake website that is identical to the real bank site and uses the fake site to steal credit card and other identity information from the bank's customers.

With the victim bank to help them, the NCFTA traced the attack to its source and identified what measures they could take to mitigate the effects of this attack. With the help of the NCFTA, the bank was able to send "cease and desist" letters to the Internet service providers hosting the fake sites in order to have the sites shut down.

InfraGard is an alliance between the FBI and the public whose mission is to prevent attacks, both physical and electronic, against critical infrastructure including, but not limited to banks, hospitals, telecommunications systems and the Internet. InfraGard has over 14,800 private sector members spread across 84 local chapters throughout the United States. These private sector partners represent the full spectrum of infrastructure experts in their local communities.

FBI Agents assigned to each chapter bring meaningful news and information to the table such as threat alerts and warnings, vulnerabilities, investigative updates, overall threat assessments and case studies. The FBI's private sector partners, who own and operate some 85 percent of the nation's critical infrastructures, share expertise, strategies, and most importantly information and leads that help the FBI track down criminals and terrorists.

The Internet Crime Complaint Center, IC3, is a joint initiative between the FBI and the National White Collar Crime Center (NW3C). Located in West Virginia, a short distance from the NCFTA facility in Pittsburgh, the IC3 serves as a clearing house for cyber crime incidents reported by both individuals and business.

The 1C3 receives, on average, 25,000 reports of cyber crime incidents each month. By analyzing these complaints for commonalities and trends the 1C3 is able to develop cases that have a national impact. These cases are then referred to local, state, or federal law enforcement agencies for investigation. As with the NCFTA, the 1C3 also focuses on partnerships with business as the most efficient and effective way to combat cyber crime.

In 2002 the 1C3 began an initiative online retailers combat fraud from re-shipping scams. The initiative known as Retailers and Law Enforcement Against Fraud (RELEAF) brought together teams of analysts at the 1C3 and e-commerce businesses to identify fraudulent online purchase which were being shipped by domestic re-shippers to destinations overseas.

In one 30-day period, the RELEAF initiative resulted in 17 arrests, 14 controlled deliveries, the recovery of $340,000 in stolen merchandise, and the recovery of over $115,000 in counterfeit cashier's checks.

Chairman AKIN. Steve, you are about out of time.

Mr. MARTINEZ. Okay. Thank you. I would be happy to answer any other questions about our initiatives.

[Mr. Martinez's testimony may be found in the appendix.]

Chairman AKIN. Thank you. Because of the vote being called, I am going to have to scoot out. I would like to start by asking a question. I do have some staff here that can take a few notes. I guess the first thing that I am interested in, and all of you are immersed in this whole situation on a day-to-day basis, we just touch on it and run to lots of other things.

I would like to know your assessment of how big a problem we have, first of all, and how do you measure that. Then the second thing is within the scope of where we have a problem, do those things tend to cluster in certain areas? Are there a couple of certain particular places such as identity theft or something where that is the majority of what we are concerned with. So I am interested in scoping the problem and getting a little bit of a sense as to what categories those things are in. If you could answer that.

Then I am going to turn the chair over to Ms. Bordallo. I have got probably about half an hour of voting or so so I would expect you will adjourn and we will call a second panel at that time. Thank you very much.

Ms. BORDALLO. Thank you very much, Mr. Chairman Since I represent the territory of Guam we don't vote on the floor. That is one thing I wish we could but the territories do not have that privilege. We vote in committee but not on the floor.

I think we will take the two questions that the Chairman presented and we will begin with Mr. Larry Johnson. What would your answer to those two concerns that he has.

Mr. JOHNSON. What the Secret Service has seen a large percentage of the time is that attacks on businesses, whether small or large, are typically for financial gain. What we have also seen is identity theft being a component of not only assuming someone's identity through intrusions, social engineering and other methods. That is very prevalent of the major attack.

However, a recent trend is that if you can bypass the identity theft and go right to an institution that stores financial data. We have seen that now more common than ever that if you can bypass the identity theft and steal credit card numbers and other financial data, account takeovers. We have seen alarming rate of account takeovers, specifically retirement accounts because that is where the largest amount of money people usually have.

Ms. BORDALLO. So you would consider that the biggest problem?

Mr. JOHNSON. Yes.

Ms. BORDALLO. All right. Next would be Mr. Steven Martinez. Can you answer the question that the Chairman presented?

Mr. MARTINEZ. Sure. I think what we are seeing in the FBI is we are looking at cyber crime across the entire spectrum is a convergence of the hackers on the one side that we used to see as kind of stovepiped in doing their own thing for bragging rights and that type of thing, and the cyber frauders on the other.

They are now meeting in the middle. They are now leveraging each other's knowledge and it is all for profit just like Mr. Johnson mentioned. That is really a change that we have seen over the last

couple of years and it isbeing facilitated by automation in the way that these hacks are conducted.

I mentioned botnets in my testimony. They give a standoff capability to cyber fraudsters and hackers where they can perpetrate frauds against Americans from anywhere in the world. It provides an additional challenge for us because we really have to have an international scope, international reach, in order to address these things.

But, on the other hand, small businesses have a huge part to play in this. I briefed on a very successful case targeting a botnet that was brought to us by a relatively small business in the Los Angeles area. This case was expanded and we determined that it impacted on large ISPs across the nation but the nexus of this was an attack on a small business and they brought that information forward. Outreach is an important part of this because there are some disincentives to reporting that you have been attacked and have a problem. It might put you at a competitive disadvantage. We are working very, very hard on outreach in order to get the information in. As far as the scope goes, are best estimate is we probably only see maybe a quarter at best of the reporting that we would hope to get as far as the nature of the problem. There are a lot of reasons for that. Again, there are some financial disincentives for bringing that information forward. As businesses small and large get used to the fact that the FBI and law enforcement agencies know how to work these investigations without disrupting their operations, I think we can create more good will and get more of the reporting we need to address the problem better.

Ms. BORDALLO. Thank you. Thank you. Now Lydia Parnes. What do you feel is the biggest problem facing you?

Ms. PARNES. Well, the Commission really looks at this issue from the perspective of information security across the Board. I think it would be difficult for us to kind of single out how big the problem is for small businesses but we know that information security is a major issue. The issue that we have a particular focus on is identity theft.

The Commission is charged with maintaining an ID theft clearing house and so we get the consumer complaints and the inquiries from consumers who have been subjected to identity theft. I think ultimately that is the real concern about information security. We want to promote a culture of security and we want to do it because when security is lacking, identity theft can be the result with all of the resulting injury.

Ms. BORDALLO. Thank you. Cita Furlani.

Ms. FURLANI. Thank you. I think there are a few more aspects that should be considered. One I mentioned was just the sheer complexity of how you provide security. There are too many ways that things can be breached. The things that I think small businesses and any other business need to consider is that they are frequently partnering with others. They need to have some way of determining whether their partners are maintaining secure environments. They frequently outsource and are provided some kind of software or supporting structure by other businesses and how do they measure that whether they are meeting the same level of requirements that they have set inhouse.

The whole aspect of an always on Internet, always able to be on and connected adds a complexity of understanding of how you provide the firewalls and the patches. Everything that has to be done is a difficult problem.

Ms. BORDALLO. Thank you very much. Now for my round of questions. I have one for Mr. Johnson first. I was particularly interested in a point you made near the end of your prepared testimony that Secret Service Electronic Crime Special Agent Program Officers are committed to taking preventative action to guard industry from crime in addition to their responsibilities to investigate following a crime. I would encourage the Secret Service to review ways in which its technical expertise can be shared with SBA client firms. What existing partnerships, Mr. Johnson, does the Secret Service have with SBA on cyber security?

Mr. JOHNSON. With the Electronic Crime Special Agent Program, I'll just address that first. That is a training situation that the Secret Service has probably been involved in in the last couple years. We train our agents in three levels of cyber investigators. First, the No. 1 level is the forensic investigator that actually looks at the hard drives and determines the vulnerabilities based on the electronic evidence.

The middle level of cyber investigator is the network intrusion expert who is very involved and has extensive training in network intrusions. Then that lowest level is the basic cyber investigator training program where we try to have all of our special agents go through this type of training. Obviously they cycle into other assignments but eventually in the next couple of years we hope to have all special agents in the Secret Service trained as cyber investigators.

As far as the affiliations of small businesses and large businesses, we have numerous members to our Electronic Crimes Task Forces and they are located, like my testimony indicated, throughout the United States. That's where the sharing of the information is from one small company to another and they basically talk about what is the security concern of the day. What keeps their CEO up at night.

These discussions a lot of times bring out a lot of information that they would not otherwise talk about what was previously not spoken about because I don't want to admit to you my vulnerabilities. Now we have gotten companies both large and small to talk about what their security problems are and we think that has been beneficial.

Ms. BORDALLO. So what you are telling me then about these programs, the various programs that you explained, you are partnering with the SBA? Is that what you're telling me or thinking about it?

Mr. JOHNSON. Well, I probably have to get back to you on whether or not specifically we have a partnership or an MOU. I believe they are a members of one or more than one of our task force but I can let you know for sure.

Ms. BORDALLO. I think that is the basis of my question. I think it is important that we partnership.

Mr. JOHNSON. Okay.

Ms. BORDALLO. All right. The next question I have is for Mr. Martinez. I am concerned, Mr. Martinez, that after reviewing the SBA website this morning I was unable to find any information on it regarding cyber crime and small business or information on how small businesses can contact law enforcement in the event of a suspected cyber crime.

I wonder whether a small business owner or an entrepreneur knows that it should consider contacting the FBI regarding potential cyber crime. Has the FBI ever done any coordination with the SBA to educate small companies on cyber security issues? What kinds of outreach and training programs does your agency have for small business or would such a program need to be developed?

Mr. MARTINEZ. Well, the FBI does have a formal arrangement with the SBA through a memorandum of understanding to provide support leveraging our InfraGard program and the membership to assist with a series of very specifically targeted cyber security is good business. That is what these training sessions are called that target small businesses specifically across the country.

In fact, recently there have been, or will be sessions in places from San Diego, California, Sioux Falls, Minneapolis, Casper, Wyoming, places where you might likely find smaller businesses. Again, this is an effort to leverage what we have built with InfraGard, provide both access to the membership because a lot of the best information is held in the private sector, but also to provide subject matter experts within the FBI, investigators, whatever the case may be, to participate in these training sessions if need be.

Ms. BORDALLO. I certainly think that both the FBI and the Secret Service these are partnerships and I think they should be included on the website, the SBA website. We don't find anything and I think this would be extremely helpful if you could work with them and see that this be included.

I have a question for Ms. Furlani. What are the two most important lessons you teach small business owners on computer security?

Ms. FURLANI. Vigilance. How to determine whether they are—we provide checklists and ways to understand the issue and what they need to do. Frequently they have the kinds of people that can understand what needs to be done but it is a matter of resources, how much time can be spent. We try to find simpler ways to describe what can be done and give them checklists that they can go down and determine whether all the various patches have been done and the intrusion detection zone and all these things that they need to do.

Most important is mainly being aware and being vigilant. That is probably the most important because all the other things change as the threats change. It is more important to be aware of it and be understanding of what and access to where the resources are to understand how to deal with the changing environment.

Ms. BORDALLO. And, Lydia, I have a couple of questions for you. To what extent has the FDC attempted to involve the Small Business Administration in cyber security efforts that are targeted at small businesses?

Ms. PARNES. We actually have a history of working with the SBA on frauds that are directed to small businesses and we have had a number of real successes. We have not kind of dealt with them

specifically on cyber security but we would be delighted to have them participate in OnGuard Online which is our online cyber security information.

The OnGuard Online is not marked as an FTC site particularly. You can get it through our site but we encourage others to use it and put it out there and we will definitely contact the SBA. They can take the site. They can link to it or just put it on their site as well. I think it would give small businesses very good information.

Ms. BORDALLO. But this, again, hasn't happened as yet.

Ms. PARNES. No, it hasn't. I would add that we do have federal agencies who partner on OnGuard Online as well as private industry. It is up there and it is available to anybody who wants to use it and we will seek out the SBA.

Ms. BORDALLO. Another question. Under what circumstances should a small business owner report cyber attacks to FTC? What would be the extent of the problem before they contact you? What would the circumstances be?

Ms. PARNES. Well, certainly the FTC is one place that a small business can contact about a cyber security attack. The information that we get goes into a database that is available and actually is downloaded onto the FBI database that Mr. Martinez talked to. The Secret Service has access to our database as well.

A small business could easily contact the FTC. We would take all of the information. We would put it in our database and it would be available to law enforcers, both federal law enforcers and also law enforcers on the local and state level. The FTC does not have any criminal authority, however. So many of these attacks are criminal in nature.

Ms. BORDALLO. What would you say the frequency of inquiries are? Any of you could answer that.

Mr. MARTINEZ. On the IC3, the Internet Crime Complaint Center complaint intake runs about 25,000 complaints a month. That is individual consumer complaints. That doesn't include aggregated information that we get from private sector partners.

Ms. BORDALLO. That is a staggering number. Let me see here. I think that is pretty much all the questions. We are trying to extend this before we call up the second panel. Oh, yes. I have one for the FBI. What is the most common roadblock you encounter when tracking down cyber criminals?

Mr. MARTINEZ. I think the biggest challenge for us right now is the international nature of cyber crime because going across the world you have different relationships with different countries and different levels of cooperation so we put an awful lot of effort into developing and firming up those relationships in places where we haven't had a presence before.

You know, former Soviet states, the Far East. We have a legal attache program where we have a presence in many, many foreign countries but we found that we actually have to put people on the ground to work with some of these countries that haven't developed their legal systems or their capabilities to address cyber crime so that has been a huge challenge. It is really a change in the way we do business because we used to focus mostly on domestic crime

problems but it really is a completely international global crime problem now.

Ms. BORDALLO. Secret Service, how would they respond?

Mr. JOHNSON. I would agree with Mr. Martinez. The only thing I would add is that there is a different scam every day. I become briefed on the latest and greatest and it is always something added to an existing scam on the Internet. It is a more sophisticated from phishing to pharming more sophisticated and that is just one example of trying to stay one step ahead or at least equal with the bad guys.

Ms. BORDALLO. Can you share with us what is the latest scam so we are ready for it?

Mr. JOHNSON. I think I kind of mentioned the account takeovers are very prevalent. You kind of put me on the spot with the latest.

Ms. BORDALLO. You know we have to be up to date here.

Mr. JOHNSON. I understand.

Ms. BORDALLO. Thank you very much. I think we spoke about that, the small businesses to protect against inside. You mentioned vigilance which is very importance.

Ms. FURLANI. And how best to apply their scare resources. Which vulnerability should they work on? Some kind of prioritization.

Ms. BORDALLO. Can small businesses employ adequate security measures with their limited resources? What would the cost of that be? You are talking very limited resources.

Ms. FURLANI. Again, if you know—if you have access to how to do it you can make choices as to what is the most important way to close the door and where you apply your resources. Obviously it is easier when you have a larger budget. You are using a smaller percentage of it but education and awareness and I think that is what you are focused on today is where the resources are that they can make use of.

Ms. BORDALLO. And who provides—who can provide that?

Ms. FURLANI. Our website has a lot of information and I think each of the other agencies do.

Ms. BORDALLO. But technical assistance?

Ms. FURLANI. Technical assistance is generally where they are going to be getting it from a vendor of some sort. There again, they need to have enough understanding of what they are hiring and what risk they are taking there with partners, vendors. Every time you add someone else there is another vulnerability risk.

Ms. BORDALLO. That is correct.

Ms. FURLANI. Being aware of that.

Ms. BORDALLO. We want to thank all of you for appearing before the Committee today and we appreciate all your testimony and certainly we take it into account. I would like to excuse you and bring on the second panel. Oh, we will recess for a short time until we bring up the second panel.

[Whereupon, at 3:04 the Subcommittee adjourned until 3:24 p.m.]

Chairman AKIN. The Committee will come to order. Sorry about breaking things up here. I think we are prepared to go with our second panel if I am not mistaken. Ari Schwartz. Is that correct?

Mr. SCHWARTZ. Ari, yes.

Chairman AKIN. Ari. Okay. Deputy Director of Center for Democracy and Technology, Washington, D.C. You have five minutes, please, Ari.

Mr. SCHWARTZ. Thank you.

STATEMENT OF ARI SCHWARTZ, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. SCHWARTZ. Thank you. Mr. Chairman, Madam Ranking Member, thank you for holding this hearing on cyber security and inviting the Center for Democracy and Technology to testify. CDT hopes that this marks the beginning of the Subcommittee's interest in the important issues of information security and its impact on small business and consumers.

Much as been written and said about the Internet as a revolutionary platform for human interaction. Indeed, the Internet levels the playing field for individual speakers and small businesses. It is a cheap and effective way to reach around the world.

There are many factors that make the Internet unique among communications tools but its strength has always been it is open, decentralized, and user-controlled nature. As such, the medium inherently has the potential that promotes democracy and entrepreneurial ideas. However, the Internet's strength is also one of its weaknesses.

Just as networking and interconnectivity allows for unprecedented sharing of ideas, those factors also expose the medium to a growing number of threats such as viruses and spam and phishing spyware. Individually these attacks are dangerous enough but taken together they have begun to chip away at the trust Internet users have in the medium.

A recent survey done by Consumer's Union has indicated that 25 percent of consumers have stopped making purchases online and another 29 percent have cut back on their online shopping because of concerns about identity theft alone.

To address these dangers we must ensure both that our proposed solutions get to the root of the problem and that those solutions don't inadvertently harm the essential nature of the medium. To reach these goals we must understand the motivation and character of the threats. Although popular portrayals of Internet criminals continue to focus on young hackers, vandalizing websites, or launching denial of service attacks to gain notoriety among their peers. Most of the real threats today are driven by financial gain, as we said, by the FBI and the Secret Service in the earlier panel.

It is easy to get lulled into the belief that these are new threats because of the new terminology like phishing with a "ph" or spyware, but in reality they are for the most part typical fraud cases that we have seen offline for years and years. In our research into consumer complaints EDTS found these attacks are generally driven by five types of financial motivation.

(1) Identify theft to consumers and businesses.

(2) Corporate espionage, that is, taking confidential information.

(3) Advertising software that provides pop-ups financially motivated because companies are paying affiliates to install software onto users computers and often do so without consent.

(4) Fraudulent marketing schemes like those that we become used to in our e-mail boxes every day. And,

(5) Extortion where consumers or business data or an entire machine is held ransom in one way or another.

We are also seeing more attacks that rely on multiple techniques also known as blended threats that are uniquely targeted to a specific type of user. The New York Times recently reported that large gangs of criminals in Brazil and Russia are using virus-like techniques to install password crackers that only work on certain banking websites. This demonstrates not only the new skill of the criminals but also the international nature of the threat.

These attacks have magnified impact on small business because many small businesses suffer from those attacks of the consumers as well as those aimed at businesses. Also, while large enterprises can afford spare capacity in the form of additional computers and servers, many small businesses do not have that luxury.

Because of the changing nature of the threats, it is important that security programs continue to improve. Computer security companies have become experts at finding problems and distributing information about whatever malicious programs caused the problem, but they are only just beginning to build and test programs that stop malicious software at the first signs of bad behavior even before the names of those programs are known.

Finally, it is essential that we address the financial motivation of these threats as we have in offline fraud. This is not as easy as it sounds because the Internet models pass information to the hands of so many players and across borders as well. CDT is currently in the process of documenting how large and respected companies are unsuspectingly supporting unfair and deceptive practices of their partners. Yet, we must get beyond all these difficulties and find the sources of funding and cut it off or risk losing the potential of the Internet for future generations.

Thank you again for having me here and I look forward to your questions.

[Mr. Schwartz's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Ari. Right on time there. Next we have Enrique Salem, Senior Vice President, Security Products & Solutions from Symantec Corporation from California. Thank you for coming the distance here, Enrique.

STATEMENT OF ENRIQUE SALEM, SYMANTEC CORPORATION

Mr. SALEM. Thank you, Chairman Akin, and Ranking Member Bordallo for giving me the opportunity to testify at today's hearing on the state of small business security and cyber economy. I am hopeful that my remarks will provide the Committee with a comprehensive overall of the U.S. small business cyber threat landscape. I also hope to give you some thoughtful insights on the many security challenges small business owners face in today's growing digital economy. I look forward to responding to the Committee's questions following my remarks.

I come before you today representing Symantec Corporation. We are the fourth largest software company in the world and we help our customers to protect their information and we provide them solutions around security and availability and integrity of their data.

As the Senior Vice President for Consumer Products Business Unit I am responsible for both the consumer market and the small business segment. Prior to joining Symantec I was the CEO of Brightmail, Inc., a leading provider of anti-spam solutions so I am able to talk to you about some of the key challenges that small businesses face when they try to deal with spam. I also provided comments to Congress on the issues surrounding the CAN SPAM Act.

Last week Symantec released its ninth Internet Security Threat Report which is widely acknowledged to be the most comprehensive analysis of information regarding security activity for today's economy. The report includes an analysis of network based attacks including those on small businesses with a review of known threats, vulnerabilities, and security risks. We have been providing this report on a semi-annual basis since 2002.

The last two Internet security threat reports found that small businesses have consistently been in the top three most targeted groups for cyber attacks. Cyber criminals have found that small businesses are less likely to have a well-established security infrastructure making them more vulnerable to attacks.

Symantec has also sponsored the first comprehensive study of its kind analyzing the state of information security readiness in the U.S. small business market. The July 2005 study conducted by the Small Business Technology Institute surveyed more than 1,000 businesses and found that information security is a high priority for small business owners. But it also showed a lack of appreciation of the true economic impact of information security incidents and a lack of knowledge around cyber threats.

I would like to submit this report with the Chairman's permission.

Chairman AKIN. Without objection.

Mr. SALEM. Some key findings that we found in the report are as followed. While over 70 percent of small businesses consider information security a very high priority, they are not increasing their investment and protection. The study revealed that small businesses demonstrate an alarmingly complacent and passive attitude to information security.

A majority of small businesses, 56 percent, have experienced at least one security incident in the past year and small businesses make overwhelmingly reactive purchase decisions when it comes to Internet security with 35 percent increasing spending on security products only after their business has been compromised or attacked resulting in a loss of data or corruption.

It is difficult to quantify the impact of cyber crime but according to the FBI's 2005 Cyber Crime Survey costs today are around $67 billion to U.S. firms over the last year. Additionally, the FTC found that the identity thief cost businesses $48 billion and last year consumers $680 million in losses.

But more damaging than the loss of money is the loss of trust and confidence by consumers in the Internet economy. With so much of the nation's small businesses depending upon the Internet, we can't risk losing the public's confidence in doing online transactions with small businesses as it is essential that they have the right resources to protect themselves.

Symantec continues to play an instrumental role in protecting small businesses through the security solutions we offer and our education and awareness efforts.

For example, Symantec is a major sponsor of the National Cyber Security Alliance, or the NCSA, a non-profit which educates small businesses and consumers how to stay safe online. The NCSA website, staysafeonline.org, is a useful resource for small businesses and partners with the Department of Homeland Security, FTC, Small Business Administration, NIST, and many others on several initiatives including the small business training workshops lead by NIST.

In addition to its sponsorship of the NCSA, Symantec has created several tools, including educational books and CD-ROMs to address the unique needs of small businesses. We have copies of these materials available at today's hearing that Symantec has also developed in a wide-range of areas to help protect data that small businesses find critical to run their businesses.

We must focus on increasing cyber security awareness, educating and enabling small businesses to properly assess their true level of risk and encouraging them to take the necessary and preventative and corrective measures.

Symantec looks forward to continuing to work in partnership with the private sector and Congress to conduct research and create tools that lead the way in providing U.S. small businesses with the right resources they need and deserve to truly secure and prosper in today's high-tech global economy.

Thank you again, Chairman Akin, and Ranking Member Bordallo, allowing me to testify today in front of the House Small Business Subcommittee on Regulatory Reform and Oversight.

[Mr. Salem's testimony may be found in the appendix.]

Chairman AKIN. Thank you very much, Enrique. Appreciate your perspective.

Next is Dr. Burton KALISKI. Is that right?

Dr. KALISKI. Kaliski, sir.

Chairman AKIN. Kaliski. You are the Vice President of Research for RSA Security, Chief Scientist, RSA Laboratories from Bedford, Massachusetts.

STATEMENT OF DR. BURTON S. KALISKI, JR., RSA LABORATORIES, RSA SECURITY

Dr. KALISKI. Chairman Akin and Ranking Member Bordallo, I am honored to be with you today. You might wonder what the three letters RSA stand for. They are the initials of three inventors of a very widely-used encryption algorithm developed in 1977 at MIT with federal research funding.

We have a conference held annually on the west coast which now attracts 14,000 attendees and at the most recent conference Robert Muller spoke and said that, "While the Internet has become a growth engine for business, it has also become a global target for cyber criminals." He is exactly right and this is a dilemma for small businesses because, on the one hand, you want to go online to expand your business opportunity. On the other hand, when you go online you face tremendous threats and small businesses don't have the IT security departments to help them but there is hope.

We need to look at what is an adequate level of security for a small business or any business. We believe that security ought to be commensurate with the value of the data as well as the resource being protected. Just as you don't shred every piece of paper, you don't need to encrypt every file but you need to be shredding and encrypting sensitive information. Just as you don't lock every door, you don't need to have strong access controls to every file but those that are sensitive need that appropriate level of protection.

Now, traditionally the protection for access to information has been a password and it is recently that across many industries people have realized it is finally time to do something better. But what is there that is better than a password?

Well, at the RSA conference this year Bill Gates was one of the speakers and he said, to paraphrase, that the era of passwords is over. Organizations are looking at many technologies for making it easier to use stronger security but we again have a dilemma. If you have strong security that is very strong but not easy to use, you really have no improvement at all. Great security is good to have if you can use it.

There has been a substantial increase in the focus on usability and I would like to highlight several ways that is taking place. One is that vendors are finding ways to make security more usable across the industry as a whole. You may have different interfaces on every site you interact with, a different way of providing your password, a different way of answering questions about your account.

You may have ways that you can reset your password in one case and in another case it is different but industry is working to standardize and harmonize these approaches so that users have a consistent experience. Users also have many opportunities to increase their security with the devices that they already have.

We are all carrying mobile phones. Couldn't that be used someway to enhance our security experience if we could just connect that with the places at which we do business. That would certainly simplify the situation for a small business rather than having to find some unique solution to put security in the user's hands. And vendors including my company are looking at many ways like this.

Now, the third point, though, is that you basically need it to be a crypto-engineer, and I wish I could tell you more about that career because it is fascinating. You needed to be a crypto-engineer to put security in your products. Up until recently you had to know details of every algorithm and acronym and so forth. Well, that is changing. Vendors are finding ways so that you can put encryption in and other features of security just based on policy. You say, "Here is the kind of data I have. Please encrypt it," and it is done and it is managed well.

Security appliances are another example. You don't need an IT security department to enhance your security. You can plug in a device that is ready to go into your network and it enhances your security. Finally, IT vendors are working on improvements to the user interface because, after all, that is the last and the weakest link. How does the user know that he or she is more secure? Well, there are improvements on web interfaces that help you to see when you are secure and when you are not.

In all of this the public and private partnership is essential. As my colleague mentioned, the National Cyber Security Alliance is an important player. RSA Security has also been invested in that organization. We encourage others to take part in it.

We are also interested in the area of breach notification legislation. I understand that the House and the Senate are both working in that area. We consider it important as an incentive and reward to businesses that apply best practices, that those best practices are recognized in terms of a safe harbor provision.

To conclude, just because you are a small business doesn't mean the criminals aren't out to get you as well. You have valuable resources. Just because you are a small business doesn't mean you can't do anything about it. There are tools, the built-in security into many products, the tools for encrypting data more easily.

You know, RSA Security used to be a small business and at RSA Laboratories we maintain that entrepreneurial perspective. We look forward to working with this Committee on Small Businesses for a safety and more secure economy.

[Dr. Kaliski's testimony may be found in the appendix.]

Chairman AKIN. Thank you. Very well done. Thank you very much.

Our next guest is Roger Cochetti?

Mr. COCHETTI. Cochetti.

Chairman AKIN. Cochetti. Your son Andrew is supervising this operation as well I understand.

Mr. COCHETTI. Thank you very much.

Chairman AKIN. You the Group Director of U.S. Public Policy, Computing Technology Industry Association from Arlington.

Mr. COCHETTI. Yes, sir.

Chairman AKIN. Thank you, Roger.

STATEMENT OF ROGER COCHETTI, U.S. PUBLIC POLICY, COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION

Mr. COCHETTI. Thank you, Mr. Chairman Thank you Ranking Member Bordallo. Thank you both for your warm welcome for my 13-year-old son Andrew for whom the subject of cyber security I can assure you is not a theoretical issue.

My name is Roger Cochetti and I am Group Director of U.S. Public Policy for the Computing Technology Industry Association (CompTIA). I am here today on behalf of our 20,000 member companies.

Mr. Chairman, I want to thank you and the members of your Subcommittee for holding this important hearing on the State of Small Business Security in the Cyber Economy. We believe that your efforts to focus public attention on cyber security and small business will help American small business avoid cyber threats.

Before I continue, Mr. Chairman, I would like to ask that my written statement be submitted for the record.

Chairman AKIN. Without objection.

Mr. COCHETTI. Mr. Chairman, the Computing Technology Industry Association is the nation's oldest and largest trade association representing the information technology or IT industry. For 24 years CompTIA has provided research, networking, and partnering opportunities to its 20,000 mostly American member companies.

While we represent nearly every major computer hardware manufacturer, software publisher, and systems integrator, nearly 75 percent of our membership is made up of the small American computer companies who themselves provide integrated computer systems to small businesses which I will explain more in a moment.

As this Subcommittee knows, small business is the backbone of the American economy. Some 23 million small businesses generate over half of our GDP and employ most of the private sector workforce. Today nearly all American small businesses are dependent upon information technology and most are increasingly dependent upon the Internet. Failures in the IT infrastructure or in the Internet threaten the viability of American small business and their vulnerability to cyber threats is America's vulnerability.

The IT needs of small businesses are mainly addressed by an important segment of the computer industry called Value-Added Resellers, or VARs. These small system integrators, which are the bulk of our members, set up and maintain computer systems and networks for small businesses. VARs create and maintain the computer systems in your dentist office, in your doctor's office, for your corner store, and for your local plumber.

VARs are the front line in America's defense against cyber security threats. An estimated 32,000 VARs sell about one-third of all computer hardware sold in the United States today and most of that to small business. Because of our unique role representing America's VARs CompTIA has done a great deal to address the issue of cyber security for a small business, much of it in conjunction with governments.

We recently launched a series of regional educational programs on cyber security expressly for VARs and through them the small businesses whom they serve. In 2002 we introduced these security plus professional certification for IT professionals. It validates an IT professional's abilities in the area of cyber security and to date over 23,000 IT pros, many working for small businesses, have taken and passed CompTIA's security plus exam.

Over the past few years we have commissioned an annual survey of the state of IT security. Two-thirds of the participants in these surveys are small businesses and the results tell us a lot about the cyber threat to small business. Almost 40 percent experienced a major IT security breach within the last six months.

Human error, either alone or in combination with a technical malfunction, caused four out of every five IT security breaches. More than half do not have written IT security policies. One half have no plans to implement security awareness training for their employees outside of the IT department, nor have they even considered it. About two-thirds have no plans to hire IT security personnel and just a quarter require IT security training and a 10th require professional certification.

With our permission, Mr. Chairman, I would like to submit our most recent study for the record of this hearing. It talks a lot about what is happening in small business.

Chairman AKIN. Without objection.

Mr. COCHETTI. Based on our studies it is clear that more needs to be done to raise cyber security awareness, education training, and professional certification within the small business community.

It is also clear to anyone who understands how small businesses operate in the United States that VARs must play the central role in any effort to reach out to small business in this area. What is most needed is a Government industry partnership that takes advantage of the unique access and perspective of thousands of VARs who IT enable small business in the U.S.

Mr. Chairman, let me emphasize at this point that the most effective solutions to nearly all cyber security threats, to small business or any other IT users, do not rely on new federal or other regulations. The nature of the Internet in particular is a global network of networks that is dynamic and rapidly changing is such that Government regulations will have a limited impact.

Much more effective in dealing with threats like cyber security are technology tools, industry best practices, and consumer and business education backed up by strong law enforcement. The key role that Government agencies can and should play, aside from arresting and prosecuting criminals, is to work with industry and consumers on education, technology tools, and best practices.

We look forward to working with this Subcommittee and the relevant agencies in such a cooperative effort. Thank you, Mr. Chairman.

[Mr. Cochetti's testimony may be found in the appendix.]

Chairman AKIN. Thank you, Roger. Appreciate your testimony.

Our last witness is Howard Schmidt, President and CEO of R & H Security Consulting LLC, and former White House Cyber Security Adviser from the State of Washington.

Howard.

STATEMENT OF HOWARD SCHMIDT, R & H SECURITY CONSULTING, LLC.

Mr. SCHMIDT. Thank you very much, Mr. Chairman and Ranking Member Bordallo. Thank you for the opportunity to appear before you this afternoon.

My colleagues have done a very good job of sort of laying out the problems. I would like to spend my five minutes sort of talking about some of the things that we have seen which actually have helped improve it and some of the things that are either low cost or no cost that small and medium businesses can work with.

First I would like to frame it in saying when I look at a small business we see in three categories their IT capabilities. First, we are basically aware that their IT system is also their home computer system, the mom and pop operation, so to speak.

We have others where small and medium enterprises have dedicated computer systems, relatively small staff that basically work really hard to make the IT system run but no special expertise in security. Then the third category, the ones that actually outsource this to a service provider that basically provides them a turnkey operation.

With these categories in mind, their success depends on four things, technology, awareness and training, information sharing and, of course, we heard from the earlier panel the law enforcement capabilities.

From a technology perspective we have seen software developers invest heavily in tools and processes to reduce the number of

vulnerabilities which then make us much safer in the software we are running today. There is also now automated tools available to identify vulnerabilities, effectively the unlocked door on a computer system that can be found automatically, once again, for a low price.

The automatic updating of anti-virus applications, spyware, operating systems, things of this nature, once again, are being built into the computer systems we are running. We now see a new generation of toolbars for web browsers that turn red, green, or yellow depending on whether the site is trusted, unknown, or untrusted.

We also see new technology that is very affordable for the consumer and the small and medium enterprise with the all-in-one device where you have a hardware device that is your cable modem, firewall, wireless router, anti-spyware built in that is managed just like it would be for a large enterprise.

As Burt talked about, two factor authentication, a concept like an ATM card, something you have, something you know. It is very important for us to help secure our systems today. Also the encryption technologies are much more affordable, easier to use than ever before, and more widely accepted.

For the awareness and training, one of the issues I see with the small and medium businesses is the fact that they don't often times recognize they are and can be a target. Clearly recognizing that takes place is one of the key issues for awareness and training.

The Treasury Department released a DVD called "Identity Theft: Outsmarting the Crooks" which includes, of course, information for SNBs, The FTC, USPS, USSS, my role as a reservist with Army CID as well as other private sector groups helped put this together. It is available free of charge on the Treasury website. I might note here, if I could, I have a number of URLs or weblinks in my written testimony. I would like to just point that out. I won't repeat these things.

Of course, FTC with the Online OnGuard site, National Cyber Security Alliance, also for state and local governments working with the local Chamber of Commerce, the multi-state ISAC, Information Sharing Analysis Center, led by Will Pelgrin out of Governor Pataki's office, have put together state and territory-wide information sharing analysis.

The US-CERT provides services free of charge. The National Cyber Security Partnership was also mentioned earlier. Also there is a special guide called, "Common Sense Guide to Cyber Security" for small and medium businesses given out by the US-CERT ready.gov website, as well as the U.S. Chamber of Commerce.

On the sharing earlier we mentioned the InfraGard and the Electronic Crimes Task Force working with the local folks that actually are doing the work on a day-to-day basis. We also see information and training also take place during those organizational meetings they have.

The last piece I would like to cover briefly is the law enforcement efforts. Like any other effort, there is going to be bad actors out there. We can't escape that. With the technology, the awareness and information sharing we can help reduce the threats against the small and medium businesses but they still will see some out there.

The very nature of the crimes make them difficult to investigate so we need to make sure we currently fund particularly small, local

jurisdictions which don't have the resources to conduct these investigations without some assistance.

The International White Collar Crime Center actually is an NIJ funded project designed to help state and local law enforcement investigators investigate all types of cyber crimes, particularly, once again, targeting the audience of the small and medium enterprises.

Lastly, some quick recommendations in my last 30 seconds or so. We have seen since we have released the President's National Strategy to Secure Cyber Space that a lot of these efforts have taken place but we still see some areas. The idea of pulling the technology websites doesn't really cut it. We need to be able to provide this information. Maybe the Small Business Administration working with the U.S. Chamber and the local Chamber of Commerce to hold in-person type events to be very, very helpful.

We also basically need to make sure that when the Small Business Administration works with the loaning process you have to submit a business plan and things of this nature. Also a cyber security plan would be very helpful

With that I will wrap up my verbal comments. Once again, thank you for the opportunity and look forward to any questions that you may have. Thank you.

[Mr. Schmidt's testimony may be found in the appendix.]

Chairman AKIN. Thank you very much, Howard. You have really led into my first question. As a hard to get along with crusty old conservative, I have a natural inclination to wonder whether the Government is going to do any good and maybe make the process worse. I guess one of the things that we are investigating here, the first set of questions which I really left to be asked when I was gone was, one, how big is the problem and where is the problem? Can we define what the problem is?

Second of all, what we are looking at is is there someway we can be constructive and help and in certain places maybe we should get out of the way. I wanted to let anybody who wants a shot at that question to make recommendations because we are going to be taking notes. If there are some logical places for us to put some legislation together, we probably have a good chance of getting something done. Maybe there are some places we want to stay away from and just let industry work with it. Have at it, my friends.

Mr. SCHMIDT. If I may on the issue of scoping, just my local law enforcement as well as my experience with the FBI we don't do a good job on capturing what is really computer crime or cyber crime, particularly as it relates to the smaller organizations. We have these broad categories which don't especially do it. Fraud whether using a computer or a typewriter is still a fraud and we don't differentiate that very well.

As far as the regulation piece, once again, it is in the same category. I don't think regulation itself helps but what you do is make sure the resources are available to the Small Business Administration to do not pull technology but push technology to the constituents they work with.

Chairman AKIN. Your idea that if somebody wants an SBA loan or something, you say, "Well, if you want that, then maybe what you need to is at least ensure some level of security in your system." That seems to be kind of an incentive, I suppose, that you

could use. Is that a good idea, other gentlemen, or is that just making it harder? Our last hearing that we had was how people are having trouble getting SBA loans. They said it is taking a lot of red tape and hassle. Do we want to add another step to that or not? You tell me.

Mr. COCHETTI. Mr. Chairman, if I could go back to the broader question and then touch on the SBA loan qualification question, I think it is important to keep in mind the scale of the problem and the scale of the problem is enormous and we believe serious. All of the surveys, ours in particular, suggest that well over half of the 23 million small businesses in the United States have very little preparation for cyber threats and well over half. Half would be a modest way of looking at it.

There are many things that are needed to be prepared. Technology tools are one, training is another, and procedures are another. There are others but those are typically the three main things. You train people, need the technology, and you need the procedures. Most small businesses have none of these.

Clearly from our point of view the starting point in any discussion about what to do is awareness, education, and training. Small business until they are aware of this problem are not going to do much about it and aware of the seriousness of it and the impact it could have on them.

The outreach issue consequently is the fundamental issue, we believe, that needs to be addressed. If you think about the size of the small business segment to the American economy, however, reaching out to 23 million small businesses is not something that is going to be done through putting up another website. We have got a dozen very well organized websites that provide a lot of information. How many small business men or women do you know who spend their time searching websites to learn more about cyber security?

We need a proactive outreach effort. The fact is, however, that if we were to put on a conference a month with 100 small businesses participating in each conference, it would take us several thousand years before we would reach the small business in the United States. It is for that reason, Mr. Chairman, that we believe that the intermediaries, the VARs, are really the key to the solution.

If you go to a dentist, the next time you talk to your dentist ask him, "Who handles your computer system in this office?" The odds are almost certain that he or she will not say, "I do it myself." Almost certain they will not say some big multi-national company that we have all heard of.

He or she will say, "It is Joe's Computers down the street. These are the people who are the IT departments for small business. These are the people who have to raise the bar on the awareness. These are the education outreach programs that we believe are needed, Mr. Chairman Thank you.

Chairman AKIN. Are you saying that the Government should fund education outreach programs? Is that what you are saying, Roger?

Mr. COCHETTI. I think the Government should use every tool at its disposal and we wouldn't be adverse to Government funding for

these programs but it would not be a wise use of Government resources to try to do a conference for small business because after 3,000 or 4,000 years you might have gotten two-thirds of the way through the small business community in the United States.

Chairman AKIN. Maybe we ought to publish a couple of really good juicy scandals and scare everybody. Maybe that would be the way to do it.

Mr. COCHETTI. That unfortunately sometimes helps.

Chairman AKIN. Anybody else want to take a shot at anything that we need to do legislatively or governmentally that could be helpful?

Dr. KALISKI. Sir, a couple of comments. First on the scope of the problem, Chairman Our report clearly shows that small businesses are increasingly being targeted now by cyber criminals so the scope of the problem is only going to continue to increase. I think the second point is—

Chairman AKIN. You talked about the fact that it is increasing. Do you have a sentence or two on what the scope is itself?

Dr. KALISKI. Yes. So what we are seeing is specifically that there has been at least one incident at about 56 percent of all small businesses where their data or security has been compromised so that is more than half have had an incident in the last year so that is pretty significant.

I think the second point is we do need to provide incentives for small businesses to take action to protect themselves. You mentioned this notion of small business loans. I think that may be an incentive but we should look for other mechanisms that we can use to encourage them to secure their businesses.

I think the other thing is, as Mr. Cochetti said, I don't think we need new websites. There already are existing ones such as staysafeonline.org which I think is a fine website to leverage for providing information to small businesses. Lastly, I think the SBA just needs to take a stronger role in helping small businesses to secure their businesses.

Mr. SCHWARTZ. The one area where I think there has been some discussion about legislative initiatives is in terms of international cooperation among law enforcement. We have seen a lot of the cases we track go to the border. Some of them are simply routed through foreign servers to make it look as though it is becoming foreign because the bad guys know that law enforcement goes up to the border and that's where they end their hunt because we don't have this kind of cooperation even though they are actually located in the United States.

Although some really are, there are a growing number of threats that really are outside of the U.S. and come in and work across borders, multi-national partners in these schemes because they really are money-making schemes these days. That means they will work with whoever is willing to partner with them to make money. We have seen schemes that involve seven or eight countries sometimes.

Chairman AKIN. Thank you very much. I'll turn the questioning over now to Ranking Member.

Ms. BORDALLO. Thank you very much, Mr. Chairman My first question is to Mr. Kaliski. I got mixed signals here in listening to

some of the comments. Who do you think is best situated to handle cyber security threats, the Federal Government or private industry?

Dr. KALISKI. In think it has to be a combination of both. I don't think it should be an "or" situation. I think we definitely have to raise awareness. I think there is some knowledge out there but I think it is both private sector and Congress that need to work together.

As we mentioned, there are resources today available for small businesses. We just need to make sure that folks understand that they are there and can take advantage of them. I also think the SBA needs to take a strong role in working with the private sector and small businesses to make sure that they have the staffing and resources necessary to protect themselves.

Ms. BORDALLO. It is unfortunate, I guess, that we don't have an SBA representative here today but certainly I did hear you all speak about what you have up on your websites but when you look into the SBA website there just isn't anything that deal with this problem so it is something we are going to have to work on.

Is there is a representative from SBA? Is there anyone in the audience? Do you wish to make any comments on this? Please come forward and identify yourself for the record, please.

Ms. THRASHER. Good afternoon. I am Ellen Trasher. I am with the Office of Entrepreneurial Development at the Small Business Administration. My colleague who is here is Antonio Doss also with the Small Business Administration.

Chairman AKIN. Thank you for joining us.

Ms. THRASHER. It is our pleasure and we welcome the opportunity to be here and also to hear so many of the comments, many of which we share and understand. The dynamics within the small business community has changed dramatically over the last couple of years. The whole idea of e-commerce, doing business online, while at the same time trying to open and sustain a small business is a challenge.

Our role within Entrepreneurial Development is to educate, inform, counsel, and train small businesses to make smart business decision. We do this in a variety of ways. We work in public/private partnerships. For example, we are very active in the National Cyber Security Alliance. We work with NIST, the FBI InfraGard in offering training, and online counseling and training.

Through our resource partners such as SCORE and SBDCs we offer counseling and training both face-to-face and online. For example, SCORE has an online counseling service and if you go to www.score.org you can find at least 140 online cyber counselors with an expertise in computer security that are available 24/7 to provide you counseling and training.

We are aware of the problem. We are trying to collaborate as best we can in avenues to, again, outreach, as we were talking about. We do the training, the counseling, the awareness, and we hope to refer people to the areas for deterrents, enforcement, and remediation. Thank you.

Ms. BORDALLO. You say that this then, Ellen, is all on your website now?

Ms. THRASHER. Much of it is. In fact, I just provided the Committee with brochures that we give out. We have a collaborative agreement with Hartford and have published a whole series on risk management, of course, which cyber security is part of. The brochure and the training is available both in English and Spanish and it is on site. We are also launching a webinar that will be a self-styled tutorial training course on what we call business catastrophe of which anything, of course, that would happen to your cyber security is part.

Ms. BORDALLO. Very good. Thank you. It has been very informative and I have the material here in front of me. Thank you, Ellen.

I have a question now for Mr. Cochetti and that is you spoke about the outreach program, the education outreach. Who should head the education outreach program that you described?

Mr. COCHETTI. Delegate Bordallo, there is no question, I think, in the minds of anyone on this panel that it is that educational outreach program which is the most important thing that needs to be done. If nothing else happens, without that there will be little progress. I think certainly in our view, and I suspect most of the panelists here would agree, is that this really needs to be a Government/industry partnership.

There is simply no way the industry is going to mount an effective outreach program on its own, nor is there anyway the Government could do it effectively on its own so a partnership is what is needed. I would say there are a number of federal agencies that are already active. They have modest programs underway right now. Most of the programs that exist today are responsive. In other words, I have a website.

If anybody feels like coming to it, I have information available. What really is needed is a proactive program that goes out and it is, again, for that reason that we think these VARs are what the military planners call sort of forced multiplier. Each VAR is the IT department for about 200 small businesses. You get a VAR and you reach 200 small businesses and it is a way to deal directly with the problem. I think the fact is there are a number of federal agencies, many who are here and some who are not here, who have an interest in some programs in this area. They need to work together—

Ms. BORDALLO. With private industry.

Mr. COCHETTI. Yes.

Ms. BORDALLO. Thank you. Mr. Schwartz, in your mind should the Federal Government be focusing on enforcement of existing laws or should we be looking at new laws? If new laws and regulations are needed, what recommendation do you have?

Mr. SCHWARTZ. Well, in terms of the existing laws there are several existing laws where they should be enforced more diligently and where we need greater oversight. The Computer Fraud and Abuse Act, for example, is one that we see regularly broken, criminal statute where action can be taken.

The FTC has started to take greater actions in unfair and deceptive practices cases. We started to see more action in that area. And the Secret Service has talked about in their statute the number of places where they can bring cases under current identity theft laws.

All of those pieces need to be enforced more strongly than they are today and with an international focus. There is definitely room there. The one area where we have focused on regulation where we think it is necessary goes back to the basic Internet privacy question.

There is a general question of Internet trust and of consumer trust on the Internet today. A lot of that goes back to the fact that consumers don't understand what happened to their information and how it is shared on the Internet. There is a patchwork of laws right now for consumer information and how it is used online behind the scenes for consumers that happens online and offline as well. But in the online world consumers have this fear and they don't understand what happens to their information. In some ways it is justified. We have all sorts of different standards. There are lawyers out there that do not understand the Gramm-Leach-Bliley Banking Law and privacy when they read those privacy notices that they are sent. When you are given the privacy notices in your doctor's office, a completely different kind of notice than the financial notice that you got before. We just have this patchwork of laws out there all over the map and consumers just don't understand where their information is going and how it flows and that is starting to show up online.

That is one thing that we would like to see is sort of a leveling and understanding, a baseline standard for privacy that basically the good companies out there are following but the other companies out there that are sort of outliers are taking advantage of.

Ms. BORDALLO. That is an excellent point. Mr. Kaliski, new developments in cyber security certainly will enhance small businesses. We have all been talking about that. Are these protections affordable?

Dr. KALISKI. That is an excellent question, ma'am. the important part to look at is that as technology is developed and standardize it becomes widely available, very effectively for a large group of people. Consider the Internet as an example and over time the higher speed Internet access that has been made available to all kinds of businesses.

We are seeing a similar trend in security technology. As I mentioned, vendors are producing security tools that can be used across multiple companies so that you are able to leverage the investment that your users have already made to be secure in other places. An example, there are security tokens that are issued by banks that can potentially be used at other banks just as you would use a credit card at multiple places. The affordability will come from the common solutions available through industry standards.

Ms. BORDALLO. Thank you. Mr. Schmidt, I have just one last question. It seems to me that SBA should be playing a larger role given that if there is any agency small firms would turn to for advice it should be SBA. Would you agree with this assessment and what additional programs should the SBA sponsor to better fulfill their responsibilities to the American small businesses?

Mr. SCHWARTZ. I agree with that perspective because the small business that I talk to the first thing I do is look to where the SBA is saying, "How can I be successful?" which is what is said to do. Part of the SBA's responsibility to due diligence, as the Chairman

mentioned a few moments ago, about making it less complicated. That due diligence also goes to the cyber piece.

Some of the things they can do is not so much focus on how to investigate these things because that is often times too late for a small business. They are already out of business at that juncture so maybe working with the Internet Association Chiefs of Police and the Crime Prevention Associations to take that good material that they have just passed out to you and make sure that those are provided.

For example, if you were to call up your local police department and say, "I would like you to come to my house and my business and do a crime survey," they will come out and do it. Ask them to do that on your computer business and they won't have a clue what to do. The SBA has the expertise, the resources to work with them and provide that as a resource to local business as well as a crime prevention effort.

Ms. BORDALLO. Thank you very much. Thank you all for the information you provided.

Chairman AKIN. I just had one or two quick questions. I have got a meeting that started at 4:00 so I am going to have to scoot before long. Just a couple of thoughts. First of all, is there anybody that provides insurance to small businesses to protect them against these kinds of problems?

Mr. SCHMIDT. As a matter of fact there are. When we released the National Strategies to Secure Cyberspace a number of the major organizations, AIG, Chubb, you name them, not only provide data insurance for the data that they protect, fire and damage, all the things relative to that at relatively low cost for small business as well. The policies are there. The underwriting capabilities are there and it is just a matter of asking for it from the insurance companies.

Chairman AKIN. So if I have got a small business, I might normally have, I would think, some sort of insurance on the building if the small business were in a building that I owned. It would be sort of like the equivalent of homeowner's insurance. I might have some liability in case an employee gets in trouble. Would any of those policies typically have insurance that would protect against data security or questions that involve the cyber security in general?

Mr. SCHMIDT. As an addendum, yes.

Chairman AKIN. You have to add it? It is an extra?

Mr. SCHMIDT. You have to add it. Yes, sir.

Chairman AKIN. Okay. And then I guess I would think that if somebody is offering me insurance, then they would have an interest in seeing whether or not you have the right software installed to protect yourself, right?

Mr. SCHMIDT. That is correct, yes.

Chairman AKIN. Okay. Then I guess the second question was in terms of the VARs, they seem to be covering a lot of the sort of small business data processing side of things. Would it make any sense to give them some sort of a rating in terms of whether or not they have taken proper precautions in terms of data security?

Mr. COCHETTI. Mr. Chairman, I think a program like that would probably make sense. We have pursued programs of sort of VAR

certification or best practices, you know, VARs who are proven to be competent. It is a nonregulated, nonlicensed industry so certification of that sort is certainly an attractive idea that we have looked at and we would be more than happy to talk with the SBA or others about sort of how to pursue it but, yes. And since they are just important intermediaries thinking about that is, I think, an important aspect of this.

Chairman AKIN. Some of us would prefer to see it maybe done on an industry basis as opposed to Government basis because we have got more confidence, especially with something that is moving as fast as this is the Government has a terrible track record at being able to move quickly and keep current.

Mr. COCHETTI. Let me assure you we are 100 percent private sector and when I mention that we have been looking at certification programs for VARs, that would be an entirely private sector certification for VARs.

Chairman AKIN. Thank you all so much for coming in. Because some of you have come a long way, I want to give you the last word. Is there anybody that has something else they want to add in? We do questions but we do answers as well so anybody who wants to make a comment.

[Whereupon, at 4:15 p.m. the Subcommittee was adjourned.]

W. TODD AKIN, MISSOURI
CHAIRMAN

MADELEINE Z. BORDALLO, GUAM
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
109th Congress
Committee on Small Business
Subcommittee on Regulatory Reform and Oversight
2361 Rayburn House Office Building
Washington, DC 20515-6319

Opening Statement
March 16, 2006
Regulatory Reform and Oversight Subcommittee
House Committee on Small Business
W. Todd Akin, Chairman

Good afternoon and welcome to today's hearing entitled "The State of Small Business Security in a Cyber Economy." I want to especially thank those witnesses who have traveled long distances to participate at this important hearing.

Today this Subcommittee seeks to better understand the impact small business cyber security has on the well-being of the economy. This Subcommittee also seeks to determine the types of threats that small businesses encounter on a daily basis. According to the Small Business Technology Institute Report released in July 2005:

> If small businesses are not made fully aware of the economic impact of information security incidents, they will continue to under-invest in information security protection, and their exposure will continue to increase as their infrastructures become more complex. This increasing individual exposure, when aggregated across the many millions of small businesses in the U.S., supporting more than half of the Nation's GDP, represents an extremely high and worsening point of exposure for the U.S. economy as a whole.

Businesses do not have to sell their products online to be at risk of a security breech. They are exposed simply by being connected to the internet. The Government and large firms have dedicated information technology professionals who protect their electronic infrastructure. Small businesses seldom have either dedicated IT professionals or the resources necessary to provide adequate levels of protection.

I look forward to hearing the testimony of your witnesses to learn more of what we can do to protect small business from cyber security threats. I now yield to the gentlelady from Guam, Madame Bordallo.

Testimony of

Cita M. Furlani
Acting Director
Information Technology Laboratory

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

before the

Subcommittee on Regulatory Reform and Oversight
Committee on Small Business
U.S. House of Representatives

"The State of Small Business Security in a Cyber Economy"

March 16, 2006

Introduction

Chairman Akin, members of the Subcommittee, I am Cita Furlani, Acting Director of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST), part of the Commerce Department's Technology Administration. Thank you for this opportunity to testify today on our perspective regarding the "State of Small Business Security in a Cyber Economy." We recognize that small businesses play an important role in the U.S. economy. Since use of the Internet is critical in the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber environment cannot be overstated. Today I will focus my testimony on NIST's cyber security programs and activities that can assist small businesses.

NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Ensuring that business-related information is secure is essential to the functioning of our economy -- and indeed to our democracy. Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users – from small and medium enterprises to large private and public organizations including agencies of the federal government.

I will share the initiatives NIST has taken to increase the level of awareness and security best practices among small businesses. Small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier, improve productivity, and remain competitive. But they face an enormous challenge in protecting their information in a cyber environment.

Since nearly 99 percent of all U.S. businesses are small or medium-sized[1], a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house very sensitive personal information including healthcare or financial information. Many small businesses also provide services to our federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which we all operate, it is vital that this important sector of our economy be aware of the risks and take appropriate steps to ensure their systems are secure.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. Indeed, the risks to our systems are so complex and pervasive, that we cannot reasonably expect small businesses to be experts in all areas of security including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology.

[1] 2003 County Business Patterns. http://www.census.gov.

NIST's Current Statutory Responsibilities under FISMA

Under the Federal Information Security Management Act (FISMA), NIST was assigned the following responsibilities:

- Develop IT standards and guidelines to secure federal systems;
- Conduct research to identify information security vulnerabilities and develop techniques to provide cost-effective security;
- Assess private-sector policies, practices, and commercially available technologies;
- Assist the private sector upon request; and
- Evaluate security policies and practices developed for national security systems to assess potential application for non-national security systems.

While targeted primarily toward federal agencies, the FISMA security standards and guidelines also are used widely by other organizations, including small businesses to help ensure that the information systems supporting enterprise operations are well protected, thereby enhancing competitiveness and productivity.

A sample of some NIST guidance which is available to small businesses is listed below:

- Guide for Securing Microsoft Windows XP Systems;
- Wireless Network Security;
- Security Considerations for Voice Over IP Systems;
- Security for Telecommuting and Broadband Communications;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Systems Administration Guidance for Windows 2000 Professional;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems; and
- Risk Management Guide for Information Technology Systems.

All of these documents, as well as our ITL Bulletins, are available on our web-based Computer Security Resource Center (CSRC) (http://csrc.nist.gov) which provides a wide range of security materials and information to constituents. CSRC now has over 20 million "hits" annually. The CSRC site also contains many policies, procedures, and practices from both federal agencies and the private sector that are also advertised to the public through our publications and outreach efforts.

We have developed guidance for organizations, large and small, to maximize the security of their information systems so that they may securely conduct business transactions over the Internet. Hardware and software purchased by small businesses today are frequently installed without making any changes from the original configurations delivered by the

vendor. We are helping small businesses to understand security features and the importance of correct configuration. Even if they have taken steps to minimize the opportunity for inappropriate access by investing in firewall technology and virus protection software, they may not have correctly installed, managed, or updated those capabilities. Given the state of software insecurity today, vendors frequently issue security patches for their products. We are advising users of the importance of these patches and where to get up-to-date information and procedures for installing patches through our outreach efforts such as our website, workshops and conferences.

Interagency Collaborations

In 2002, NIST partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The 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. To expand our outreach efforts, we have also developed a Small Business Outreach Site where you can find security resources and request a workshop to be held in your local area. (See http://csrc.nist.gov/securebiz/).

For the last four years NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers providing participants with information to increase awareness of NIST resources. In addition to our work with SBA and InfraGard, NIST is also working with the National Cyber Security Alliance (NCSA) to bring more online tools to small businesses on their small business website.
(See http://www.staysafeonline.org/basics/company/company.html)

Assistance for Small Manufacturers

NIST also is raising the awareness of the importance of cyber security in the small manufacturing community. The NIST Hollings Manufacturing Extension Partnership (MEP) was created to improve the competitiveness of America's smaller manufacturers. Realizing the gap in assistance for small firms in the cyber security area after September 11, 2001, NIST MEP developed the "eScan Security Assessment." This diagnostic tool was designed specifically for small businesses to determine how well their information technology systems are protected against failure or intrusion. It asks a series of questions and provides recommendations in the following areas: computer virus protection, file permissions, computer system physical environment, backup policies and procedures, potential computer system mechanical failures, IT contingency planning, information technology and security policies, international eCommerce concerns, Internet and eCommerce, and operating systems and security concerns.

The tool provides a report that scores each of these critical security areas. The assessment report categorizes the results and offers suggestions for improvement. NIST

MEP centers then assist the small manufacturers in addressing the issues uncovered in the assessment. While the NIST MEP program focuses on manufacturers, NIST has made the tool available for use online to all small businesses at http://escan.nist.gov.

National Vulnerability Database

NIST, with support from the Department of Homeland Security, recently developed the National Vulnerability Database (NVD) that integrates all publicly available U.S. Government computer vulnerability resources and provides references to industry resources. It contains information on almost 16,000 vulnerabilities and is available on our CSRC website at http://nvd.nist.gov/. Small businesses can go to this site to learn about vulnerabilities and how to remediate them.

Software Quality

Small and medium-sized businesses, indeed all organizations, rely on the software used on their information systems. We continue to work with industry to improve the security and reliability of software. For example, we develop standards and test suites for interoperable, robust, quality web applications and products. Our test suites are being used throughout the industry to improve the quality of implementations and specifications. We develop ways to measure the effectiveness of software assurance tools, and conduct research to assess current methods and tools in order to identify gaps and deficiencies which ultimately lead to software product failures and vulnerabilities. We conduct research and development in new areas to improve the quality of software, including software trustworthiness. We work with health-related organizations to advance the deployment of the electronic health records and to facilitate the development and implementation of a nationwide health information network.

IT Product Security Configuration Checklists

The Cyber Security Research and Development Act directed NIST to produce security checklists that cover specific technologies such as application servers, database systems, domain name servers, firewalls, operating systems, routers, and web servers. The checklists, when combined with high-quality guidance and training, substantially reduce the vulnerability of IT systems to attack. After working extensively with industry, IT vendors, and other government agencies, NIST has created a security checklist repository portal and detailed technical guidance on producing checklists. Working in concert with many government agencies such as the Office of Management and Budget, the National Security Agency, the Defense Information Systems Agency, the United States Air Force, the Department of Homeland Security and the private sector, the NIST repository now has some 87 checklists with an additional 15 expected to be finalized by May 2006. The checklists can be found at http://csrc.nist.gov/checklists/. DHS has provided crucial funding to support the development of this program.

Security Focused Research

NIST's near-term effort in Internet security research is directed at working with industry and other government agencies to improve the interoperability, scalability, and performance of new Internet security systems, to expedite the development of Internet infrastructure protection technologies, and to protect the core infrastructure of the Internet.

Looking further into the future, we see the potential for new computational models to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise ultra-secure network technologies that do not depend on today's cryptographic techniques.

NIST is a key player in the research and development of biometric standards and systems. We are working with industry and other government agencies to improve the accuracy of biometric systems that utilize fingerprints, face, iris and multi-modal technologies.

With a highly mobile workforce, use of handheld devices such as Personal Digital Assistants (PDAs) is quickly becoming a necessity for small and large organizations. NIST is working in collaboration with industry to improve authentication and encryption techniques associated with these products to ensure that the user's data and wireless communications are protected.

Meeting the challenge of securing our Nation's IT infrastructure demands a greater emphasis on the development of security-related metrics, models, datasets, and testbeds so that new products and best practices can be evaluated. The President's FY07 proposed budget will support NIST's collaborations with industry and academia to develop the necessary metrics and measurement techniques that will be combined to provide an assessment of overall system vulnerability. Utilizing approaches that have been successful in characterizing effects in the physical systems, NIST will develop the necessary measurement science and technologies to secure the Nation's IT Infrastructure.

Conclusion

In summary, Mr. Chairman, the IT security challenge facing small businesses is greater than it ever has been. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power. Certainly, there is great potential for malicious activity against non-secured or poorly secured systems or for accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST will continue to develop ways to assist small businesses in their efforts to maximize capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information. We will continue our work in the areas of secure

configuration settings, product benchmarks, outreach, training, and research. The President's FY 2007 budget request would enhance those efforts.

We believe the programs and activities described today demonstrate our commitment to a more effective national cyber security environment by assisting small enterprises in protecting their assets and staying competitive in a cyber economy.

Thank you, Mr. Chairman for the opportunity to present NIST's views regarding security challenges facing small enterprises. I will be pleased to answer any questions that you and the other members of the Committee may have.

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

before the

SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

COMMITTEE ON SMALL BUSINESS

U.S. HOUSE OF REPRESENTATIVES

hearing on

THE STATE OF SMALL BUSINESS SECURITY IN A CYBER ECONOMY

March 16, 2006

I. Introduction

Mr. Chairman and members of the Subcommittee, I am Lydia Parnes, Director of the Federal Trade Commission's Bureau of Consumer Protection.[1] I appreciate the opportunity to appear before you today to discuss the challenges consumers and small businesses face in protecting their computer systems – and the information contained in them – as well as the Commission's role in promoting a culture of security.

For more than a decade, one of the FTC's top priorities has been protecting the privacy of American consumers. The Commission is committed to vigorous consumer and business education efforts, aggressive law enforcement, and global cooperation to safeguard the security of consumers' personal information. To date, the agency has brought 12 data security cases, six spyware and adware cases, more than a dozen financial pretexting cases, and over 80 spam cases. More cases in all of these critical areas are being developed.

Maintaining the security of computer-driven information systems is essential in the information age. A secure information infrastructure is required for the operation of everything from traffic lights to credit and financial systems, communications networks, and emergency medical service. The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier than ever for companies large and small to gather and use information about their customers. Small businesses that once were limited to customers walking past store fronts on Main Street USA now can reach consumers across the globe. Transactions that once were conducted face-to-face now are conducted entirely online.

---

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

These interconnected information systems provide enormous benefits to consumers, businesses, and government alike. At the same time, however, these systems can create serious vulnerabilities that threaten the security of the information stored and maintained in them, as well as the continued viability of the systems themselves. Security breaches can cause real and tangible harms to businesses, other institutions, and consumers.[2] Securing these systems against an ever-changing array of threats is challenging, particularly for small businesses.

II. The Federal Trade Commission's Role

The Federal Trade Commission is the federal government's principal consumer protection agency. Congress directed the Commission, under the FTC Act, to take law enforcement action against "unfair or deceptive acts or practices" in almost all sectors of the economy and to promote vigorous competition in the marketplace.[3] With the exception of certain industries and activities, the FTC Act provides the Commission with broad investigative and enforcement authority over entities

---

[2] *See, e.g., United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006)(FTC alleged that at least 800 cases of identity theft arose out of information compromise); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006)(FTC alleged that data security breach compromised more than 1.4 million credit and debit cards, resulting in fraudulent charges on some of these accounts). *See also* Federal Trade Commission – Identity Theft Survey Report (Sept. 2003) *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf. This 2003 FTC survey estimated that nearly 10 million consumers discovered that they were victims of some form of identity theft in the preceding 12 months, costing American businesses an estimated $48 billion in losses, and costing consumers an additional $5 billion in out-of-pocket losses. The survey looked at the two major categories of identity theft: (1) the misuse of existing accounts; and (2) the creation of new accounts in the victim's name. Not surprisingly, the survey showed a direct correlation between the type of identity theft and its cost to victims, in both the time and money spent resolving the problems.

[3] 15 U.S.C. § 45.

engaged in, or whose business affects, commerce.[4] The FTC Act also authorizes the Commission to conduct studies and collect information, and, in the public interest, to publish reports on the information it obtains.

The Federal Trade Commission's approach to information security is similar to the approaches taken in its other consumer protection efforts: it includes educating consumers and businesses about emerging threats and the fundamental importance of good security practices; targeted law enforcement actions; and international cooperation. The Commission's educational efforts include public workshops to highlight emerging issues, consumer and business education to help identify risks to personal information and promote a "culture of security," and business education to promote compliance with relevant laws. In information security matters, the Commission's enforcement tools derive from Section 5 of the FTC Act,[5] which prohibits unfair or deceptive acts or practices, the Commission's Gramm-Leach-Bliley Safeguards Rule ("Safeguards Rule"),[6] and the Fair Credit Reporting Act ("FCRA").[7] In addition, in an increasingly global economy, international collaboration is fundamental to ensuring the security of consumers' information. An online presence can allow a small business to reach customers anywhere on the globe. And businesses routinely contract for services with providers in other countries. In fact, a company's web servers may be located on a different continent from its other operations.

---

[4] In addition to the FTC Act, the Commission also has responsibility under approximately 50 additional statutes governing specific industries and practices.

[5] 15 U.S.C. § 45.

[6] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[7] 15 U.S.C. §§ 1681-1681x.

A. Workshops, Education, and Outreach

1. Security Challenges and Possible Solutions

In 2003, the Commission held a workshop that explored the challenges consumers and businesses face in securing their computers.[8] Titled "Technologies for Protecting Personal Information: The Consumer and Business Experiences," the workshop also examined the role of technology in meeting these challenges.[9]

Workshop participants included industry leaders, technologists, researchers on human behavior, and representatives from consumer and privacy groups. The panelists identified a range of challenges facing consumers, industry, and policy makers. For example, many computer users do not buy the privacy tools now on the market or, if they do, they often use these tools improperly – for example, failing to appropriately configure their firewalls, using easily-guessed passwords, or using anti-virus software and operating systems without properly updating them.

To help businesses develop better ways to protect their systems, panelists urged the adoption of a comprehensive risk-management strategy that incorporates four critical elements: (1) people, (2) policy, (3) process, and (4) technology. Panelists discussed how each of these elements plays a role in security problems and solutions. For example, companies must (1) train their *people* about the

---

[8] In May 2002, the Commission also held a workshop on Consumer Information Security. For more information, including transcripts of the workshop, *see* http://www.ftc.gov/bcp/workshops/security/index.html. For links to subsequent Commission workshops on spam, email authentication, Radio Frequency Identification, spyware, and peer-to-peer file-sharing, *see* http://www.ftc.gov/ftc/workshops.htm.

[9] The workshop agenda and transcripts are available at www.ftc.gov/bcp/workshops/technology. The Staff Report is available at http://www.ftc.gov/bcp/workshops/technology/finalreport.pdf.

threats to information systems and the steps they should take to address them; (2) develop and communicate *policies* regarding the appropriate use of information and computer systems; (3) put in place *processes* to ensure that policies are implemented; and (4) deploy *technology* effectively and securely.

2. FTC's Information Security Campaign

In addition to holding workshops, the FTC for several years has engaged in a broad outreach campaign to educate businesses and consumers about information security and the precautions they can take to protect or minimize risks to personal information. These efforts have included publication and widespread dissemination of detailed information for consumers and small businesses; publication of business guidance regarding common vulnerabilities in computer systems,[10] and responding to information compromises;[11] and speeches and presentations. Many offices in the Commission, including the Commission's Bureau of Consumer Protection, the Office of Public Affairs, and the Office of Congressional Relations, have participated in this effort to educate consumers and businesses.

Last September, the FTC unveiled an innovative multimedia campaign to educate consumers about basic computer security practices. This cybersecurity campaign, called OnGuard Online, is built around seven tips about online safety that will remain relevant even as technology evolves, as well as modules with information on specific topics such as phishing, spyware, and spam.[12] It

---

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

[11] *See* Information Compromise and the Risk of Identity Theft: Guidance for Your Business, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.pdf.

[12] *See* http://www.OnGuardOnline.gov. The seven tips are described in detail in the FTC publication, Stop Think Click: Seven Practices for Safer Computing *available at*

includes articles, videos, and engaging interactive quizzes – in English and in Spanish.[13] In addition, it provides information about where to get help, ensuring that consumers know that they are not alone as they travel through cyberspace.

The FTC created OnGuard Online with consumers in mind, but it is a valuable tool for small businesses as well. According to the Small Business Administration, the majority of U.S. firms have fewer than five employees. In many ways, computer users in small businesses are similar to home users. They use similar applications to participate in e-commerce, send email, build spreadsheets, and create presentations. Moreover, as in the typical household, often there is no information technology professional on site. It is critical that small businesses educate their employees about good computer security practices. OnGuard Online can help them do that.

OnGuard Online is branded independently of the FTC. The FTC encourages other organizations to make the information their own and to disseminate it to reach the most people. OnGuardOnline.gov has attracted over 750,000 unique users in less than six months, and the agency has distributed over 800,000 brochures and bookmarks. In addition, numerous firms and government agencies – including many small businesses[14] – are now using the OnGuard Online materials in their own internal security training programs.

---

http://onguardonline.gov/stopthinkclick.html. The seven practices for safer computing are: (1) Protect your personal information; (2) Know who you're dealing with; (3) Use anti-virus software and a firewall, and update both regularly; (4) Be sure to set up your operating system and Web browser software properly, and update them regularly; (5) Protect your passwords; (6) Back up important files; and (7) Learn who to contact if something goes wrong online.

[13] *See* http://www.AlertaEnLinea.gov.

[14] The FTC has received emails to its OnGuardOnline@ftc.gov email account from businesses that are using OnGuard Online materials in internal security training. For example, a community bank manager from New York wrote, "We feel [OnGuardOnline.gov] would be a great training tool for all of our bank employees."

The Commission's Office of Congressional Relations also has conducted outreach through constituent service representatives in each of the 535 House and Senate member offices by providing "Safe Computing" CDs to encourage incorporation of safe computing information into mailings, newsletter articles, and other communication channels. More than 100 members now host links to FTC online resources, with many devoting entire sections of their Web sites to consumer protection issues, including identity theft and information security. In the past two years, the FTC staff has also participated in more than 40 town-hall meetings about consumer protection and information security issues. Further, the agency has participated in consumer education events on Capitol Hill, including joining the Congressional Internet Caucus Advisory Committee on a series of workshops related to information security.

3. One Education Issue: "Phishing"

One specific OnGuard Online component educates computer users about phishing.[15] Phishing is a common high-tech scam that uses spam to deceive computer users into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information. These spam messages often pretend to be from businesses with whom the potential victims deal – for example, their Internet service provider, online payment service, or bank. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and then direct them to a "look-alike" Web site of the legitimate business, further tricking computer users into thinking they are responding to a bona fide request. Unknowingly, computer users submit their financial information – not to the businesses, but to the scammers – who

---

[15] *See* http://onguardonline.gov/phishing.html. For other examples of anti-phishing educational materials, *see* FTC's consumer alert: "How Not to Get Hooked by a 'Phishing' Scam," *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf.

use it to order goods and services and obtain credit.

Consumer education is a key to solving the phishing problem. Identifying individual phishers is extremely difficult; but if computer users are educated not to email financial information in response to a pop-up solicitation or email inquiry, they can protect themselves. Small businesses also can play an important role in educating their employees and customers about the importance of protecting their personal information.[16] Companies should not email their customers asking for personal information. And they should let their customers know that they will never send such a request.

B. The FTC's Efforts to Combat Spyware

Spyware is another serious threat to the security of consumer and small business data. In 2004, the FTC sponsored a public workshop entitled "Monitoring Software on Your PC: Spyware, Adware, and Other Software," and in March 2005, the Commission released a staff report based on the information received in connection with the workshop.[17] The staff report documents how spyware causes problems for businesses. Companies incur costs as they seek to block and remove spyware from the computers of their employees. Employees are less productive if spyware causes their computers to crash or they are distracted from their tasks by a barrage of pop-up ads. Spyware

---

[16] *See* Jon Swartz, *Phishing Scams Aim to Bilk Smaller Prey,* USA Today, March 13, 2006 at 1B (noting that phishing scams increasingly are targeting regional credit unions and local banks).

[17] The agency received almost 800 comments in connection with the workshop, and 34 representatives from the computer and software industries, trade associations, consumer advocacy groups and various governmental entities participated as panelists. The workshop agenda, transcript, panelist presentations, and public comments received by the Commission are available at http://www.ftc.gov/bcp/workshops/spyware/index.htm. The FTC Staff Report, Monitoring Software on Your PC: Spyware, Adware, and Other Software, released March 2005, is available at http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

that captures the keystrokes of employees could also be used to obtain trade secrets, consumer data, and other confidential information from businesses.

One of the principal conclusions of the FTC staff's report was that active enforcement of existing consumer protection laws can help prevent the spread of spyware. Using the FTC Act's grant of broad authority to challenge unfair or deceptive acts and practices, the Commission launched an aggressive law enforcement program to fight spyware. To date, the FTC has filed six cases addressing spyware and adware and more cases are under investigation.[18]

The staff report emphasized that better technology needs to be developed to protect computer users from spyware. Fortunately, substantial efforts are currently underway to address spyware. In response to market forces, industry is developing and deploying new technologies to assist computer users. Consumers and businesses are becoming more aware of the risks of spyware, and they are responding by installing anti-spyware products and other measures. In addition, industry is helping protect consumer privacy by developing privacy-enhancing technologies.

C. Business Data Security Practices

Regardless of how well consumers secure their own information and computer systems, their personal information may still be vulnerable if the businesses with which they interact fail to implement safeguards. Therefore, in addition to its education and outreach efforts, the Commission also has sought to encourage better cybersecurity practices by bringing law enforcement actions

---

[18] *See FTC v. Enternet Media*, No. 05-7777 CAS (C.D. Cal. filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com, Inc.*, Docket No. C-4147 (filed Sept. 12, 2005); *FTC v. Trustsoft, Inc.*, No. H 05 1905 (S.D. Tex. May 31, 2005); *FTC v. MaxTheater, Inc.*, No. 05-CV-0069 (E.D. Wash. Mar. 8, 2005); *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

against companies that fail to implement reasonable procedures to protect sensitive consumer information.

1. Section 5

The basic consumer protection statute enforced by the Commission is Section 5 of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[19] To date, the Commission has filed five data security cases based on deception, which the Commission and the courts have defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.[20] In each of these cases, the Commission alleged that the companies made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers.[21] Their security measures, however, were grossly inadequate and their promises therefore deceptive.

More recently, the Commission has used its authority under the FTC Act's unfairness standard[22] to bring cases in the area of data security. In four cases, the Commission has alleged that

---

[19] 15 U.S.C. § 45(a)(1).

[20] Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), *reprinted* in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the Commission's Deception Policy Statement.).

[21] *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[22] The FTC Act defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably outweighed by countervailing

the failure to take reasonable security measures to protect sensitive customer data was an unfair practice in violation of the FTC Act.[23]

One of the FTC's most recent law enforcement actions arose from ChoicePoint's high-profile breach that occurred last year.[24] According to the complaint, ChoicePoint's failures allegedly allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. The FTC alleged that at least 800 cases of identity theft arose out of these incidents. The Commission obtained $10 million in civil penalties for Fair Credit Reporting Act violations (the highest civil penalty ever levied in a consumer protection case), $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures. This settlement is an important victory for consumers and also an important lesson for industry.

Through these information security enforcement actions, the Commission has come to recognize several principles that should govern any information security program.

First, a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures.

Second, in the information security area, not all breaches of information security are violations

---

benefits to consumers or competition." 15 U.S.C. § 45(n).

[23] *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006); *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

[24] *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006).

of FTC law – the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances.

Third, there can be law violations without a known breach of security. Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur before they take action. Companies have a legal obligation to take reasonable steps to guard against threats before a compromise occurs.

Finally, the risks companies and consumers confront change over time. Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustments to reduce these risks.

2. GLB Safeguards Rule

In addition to enforcement authority under Section 5 of the FTC Act, the Commission also has responsibility for enforcing its Gramm-Leach-Bliley Safeguards Rule, which requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.[25] The Safeguards Rule is an important

---

[25] 16 C.F.R. Part 314, available online at http://www.ftc.gov/os/2002/05/67fr36585.pdf. Pursuant to Section 501(b) of the Gramm-Leach-Bliley Act, the federal banking agencies have issued similar security guidelines that apply to the financial institutions they regulate. *See* Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Parts 30, app. B (OCC); 208, app. D-2 and 225, app. F (Board); 364, app. B (FDIC); 570, app. B (OTS).

enforcement and guidance tool to ensure greater security for consumers' sensitive financial information.

The Rule requires covered financial institutions to develop a written information security plan that describes their program to protect customer information. Due to the wide variety of entities covered, the Rule gives each company the flexibility to develop a plan that takes into account its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

The Commission has issued guidance on the Rule[26] and met with a variety of trade associations and companies to promote compliance. To date, the Commission has brought three cases enforcing the security requirements of the Safeguards Rule. [27]

Safeguarding customer information makes good business sense. In testimony on data security,

---

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

[27] *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (April 12, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005).

the Commission has recommended that Congress consider whether all companies that hold sensitive consumer data should be required to take reasonable measures to ensure its security.[28] When a small business shows that it cares about the security of customers' personal information, it increases those customers' confidence in the company. Developing a plan is a good business practice for any company that handles consumer information such as names, addresses, account numbers, or Social Security numbers.

3. The Disposal Rule

When a business disposes of information, it should do so in a secure manner. This is particularly true when handling or disposing of credit reports and similar consumer reports. Pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"),[29] the Commission recently issued the Disposal of Consumer Report Information and Record Rule ("Disposal Rule").[30] The Disposal Rule is designed to prevent unauthorized access to sensitive consumer report information by requiring all users of the reports to dispose of them properly – and not, for example, leave them lying in a dumpster available to identity thieves. Like the Safeguards Rule, the Disposal Rule contains a flexible standard – "reasonable measures to protect against unauthorized access" to the information being disposed of. However, the rule also cites some specific examples of "reasonable

---

[28] *See* Prepared Statement of the Federal Trade Commission before the Committee on Commerce, Science, and Transportation of the United States Senate, on Data Breaches and Identity Theft (June 16, 2005), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[29] On December 4, 2003, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was enacted. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified at 15 U.S.C. § 1681 *et seq.*). Many of the provisions amend the Fair Credit Reporting Act. 15 U.S.C. § 1681 *et seq.*

[30] 16 C.F.R. Part 382. *See* www.ftc.gov/os/2004/11/041118disposalfrn.pdf.

measures," including burning, pulverizing, and shredding papers, and destroying or erasing electronic media, so that they cannot practicably be read or reconstructed. In order to help businesses comply with the Rule, the FTC released a business alert on the Disposal Rule in June 2005, when the Rule took effect.[31] Even when companies are not required to comply with the Safeguards Rule and the Disposal Rule, their principles provide valuable guidance for protecting sensitive consumer information.

D. International Efforts

The Internet and associated technology have created a global community. Thus, in addition to its law enforcement and education efforts, the Commission has taken an active international role in promoting cybersecurity. The Commission is joining with its neighbors in the global community in this important effort to educate and establish a culture of security.

Last June, the FTC submitted a report to Congress recommending legislation called the US SAFE WEB Act – Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers across Borders.[32] The proposed legislation would enable the FTC to share key information with foreign partners, assisting international law enforcers in pursuing security breaches in their countries that impact U.S. consumers. The legislation also would help the FTC fight deceptive spam and spyware by allowing the agency to investigate more fully messages transmitted through facilities outside the United States.

---

[31] *See* http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.pdf.

[32] FTC, The US SAFE WEB ACT: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress (June 2005), *available at* http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf. Senator Gordon Smith introduced S. 1608, the "US SAFE WEB Act," on July 29, 2005. The bill was unanimously reported out of the Senate Committee on Commerce, Science, and Transportation on December 15, 2005.

E. Hearings on Global Marketing and Technology

In 1995, the FTC held hearings for government policymakers to consider the risks presented by rapidly evolving technologies such as the Internet and to formulate policies to address these risks. This February, the agency announced that in November 2006, a decade after the original hearings, the FTC once again will bring together experts from the business, government, and technology sectors, as well as consumer advocates, academicians, and law enforcement officials to explore the ways in which technological convergence and the globalization of commerce impact consumer protection. The new hearings will examine changes that have occurred in marketing and technology over the past decade, and garner experts' views on coming challenges and opportunities for consumers, businesses, and government. The FTC hopes to receive significant input from the small business community as it plans for, and holds, those hearings.

III. Conclusion

Consumers and businesses must be vigilant about data security in the global information-based economy. The Commission is committed to continuing its work promoting security awareness and sound information practices through education, enforcement, and international cooperation.

STATEMENT OF LARRY D. JOHNSON

Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Before the Committee on Small Business
Subcommittee on Regulatory Reform and Oversight

U.S. House of Representatives

March 16, 2006

Mr. Chairman, I would like to thank you, as well as the distinguished ranking member, and other members of the subcommittee, for the opportunity to address you today on the role of the Secret Service in enforcing U.S. cyber security laws, as well as our training and awareness outreach programs for state and local law enforcement.

Although the Secret Service is most widely known as the agency that provides physical protection to our nation's leaders, our history is rooted in our investigative mission. Established in 1865 to investigate rampant post-Civil War counterfeiting, our investigative mission has broadened substantially, particularly as our nation's financial payment systems have evolved from physical currency to credit and debit cards to Internet-based banking and digital currency. With this evolution, the Secret Service has adapted its investigative methodologies to accommodate the increasingly sophisticated systems we protect. Our formula for success in the investigative arena is centered on the trusted partnerships we have formed with other state, local and federal law enforcement agencies, private industry, and academia in our efforts to thwart attempts by criminal organizations to exploit our financial infrastructure.

With the passage of the Omnibus Spending Bill Anti-Crime Package in 1984 (P.L. 98-473), the Secret Service was provided with statutory authority to investigate a wide range of financial crimes. This includes jurisdiction over investigations involving false identification fraud under 18 U.S.C. §1028; access device fraud under §1029; and computer fraud under §1030. These three statutes encompass the core violations that comprise the technology-based identity crimes that have proliferated in recent years. Over the last two decades, the Secret Service has conducted more than 733,000 financial fraud and identity theft investigations involving these statutes which led to the prosecution of more than 116,000 individuals for violating them.

The rise in e-commerce, Internet banking, and other online financial transactions has intensified competition within the financial sector. Legitimate companies have discovered the profitability of data warehousing, data mining, and data brokerage. E-commerce has led to a dramatic rise in the collection and analysis of consumer data such as Internet purchases, credit card sales, and other electronic transactions. The interest in this data has led to its collection within the direct marketing industry. This wealth of available personal information creates a target-rich

environment for today's sophisticated criminals, many of whom are organized and operate across international borders. But legitimate business can provide a first line of defense against identity crime by safeguarding the information it collects. Such efforts can significantly limit the opportunities for identity crime.

More sophisticated criminals obtain information from company databases and web sites. In some cases, the information obtained is in the public domain, while in others it is proprietary and obtained through an unauthorized intrusion or by means of deception.

As technology has evolved and the use of the Internet has become commonplace, securing cyberspace has emerged as a priority. *The National Strategy to Secure Cyberspace*[1], focuses on the need for public-private partnerships in securing the Nation's critical infrastructures and improving national cyber security.

In support of this initiative, the Secret Service and the United States Computer Emergency Readiness Team (US-CERT), located in Washington, D.C. and in Pittsburgh, Pennsylvania at Carnegie Mellon University, collaborated on a groundbreaking project known as the Critical Systems Protection Initiative. This initiative led to the Insider Threat Study (ITS), which was a behavioral and technical analysis of computer intrusions by organizational insiders in various critical infrastructure sectors. Examining incidents that occurred over a ten-year period and involved employees who caused harm to their organizations via a computer or system/network, the ITS provided insight into both the activities of the insider(s) and the vulnerabilities that were exploited. This project resulted in several key findings, including: most perpetrators used remote access to carry out a majority of the attacks; the majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks; the majority of the insider attacks were only detected once there was a noticeable irregularity in the information system or a system became unavailable; and, when hired, the majority of insiders were granted system administrator or privileged access, but less than half of all of the insiders had authorized access at the time of the incident. Copies of the ITS can be found at the Secret Service website at www.secretservice.gov.

Mr. Chairman, in response to the increasing surge of electronic crimes, and also in support of *The National Strategy to Secure Cyberspace,* the Secret Service has developed, improved upon and expanded a highly-effective formula for combating high tech crime – a formula that was successfully developed by our New York Electronic Crimes Task Force (ECTF). The New York ECTF, created in 1995, established an information-sharing conduit where state, local and federal law enforcement, private industry, and academia came together in a collaborative crime-fighting environment in which the individual resources of the participants were combined to make a significant impact on the prevention of electronic crimes. The New York ECTF is comprised of more than 250 members, including virtually every major federal, state, and local law enforcement agency in the region, myriad financial services, telecommunications and e-commerce companies, and several academic institutions. Other law enforcement agencies bring additional criminal enforcement jurisdiction and resources to the task force while representatives from private industry, such as telecommunications providers, for instance, bring a wealth of technical expertise.

[1] The National Strategy to Secure Cyberspace. (February 2003). http://www.whitehouse.gov/pcipb/.

This model has proven to be extremely successful in joining disparate agencies together to fight for a common cause.

In 2001, in recognition of the overwhelming success achieved by the New York ECTF, the USA PATRIOT Act of 2001 (P.L. 107-56) authorized the Secret Service to *"develop a nationwide network of electronic crime task forces, based on the New York Electronic Crimes Task Force (ECTF) model, throughout the United States, for the purpose of preventing, detecting and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."*

Pursuant to this Congressional directive, the Secret Service has since launched 15 such ECTFs around the country, based upon the New York model. In addition, the Secret Service has nine Electronic Crimes Working Groups – a precursor to the launching of a formal task force – and 24 Financial Crimes Task Forces throughout the country. Without question, the Secret Service's highest investigative priority is the detection, investigation and prevention of electronic crimes. Among our highly skilled personnel assigned to these cases are computer forensic examiners and network intrusion specialists.

In response to a significant shift from traditional crimes to crimes committed via the Internet, the Secret Service also established a specialized section within our Criminal Investigative Division that focuses on cyber crimes such as credit, debit and ATM card fraud; the manufacture and distribution of false identity documents; network intrusions especially for the purpose of committing online account takeovers or obtaining personal identification information and credit card account information; propagation of malicious software (malware); money laundering; and emerging crimes or criminal trends such as the use of digital / electronic currency to facilitate such crimes. This section has had significant success in coordinating global investigations, and disseminating information regarding new trends and vulnerabilities to law enforcement, as well as solidifying existing partnerships and forging new ones. Personnel from this section are regularly requested to provide presentations, join working groups, brief members of foreign law enforcement, and generate "white papers" on emerging crimes as subject matter experts.

This section provided coordination and oversight to a very significant cyber case with international ties in 2003-2004. During this case, Secret Service field agents uncovered significant vulnerabilities within the computer systems of a number of Fortune 500 companies, ranging from "back doors" into their systems to vulnerabilities that allowed hackers to enter and retrieve data without alerting system administrators. Without alarming the public, the Secret Service quietly notified each of these companies of their findings and prevented an estimated $53 million in losses through the investigation of this case. The estimated exposure to U.S. financial institutions, based on this case, was nearly $1.0 billion. This case involved the use of innovative investigative methods, and we were the first law enforcement agency to execute a wire tap on a virtual private network.

It has been our experience that the criminal groups involved in these types of cyber crimes routinely operate in a multi-jurisdictional environment. By working closely with other federal,

state, and local law enforcement, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise that bridges jurisdictional boundaries.

The Secret Service has a long standing history of sharing information and developing partnerships with state and local law enforcement. This is a result of our dual protective and investigative missions. Even in cities throughout the U.S. where there is not a Secret Service office, we typically have an established partnership based upon past protective visits. We rely on our state and local counterparts to provide assistance when a Secret Service protectee travels to various cities and towns within the United States, as well as abroad. We also provide training and assistance to these departments. Some of our educational outreach efforts have included the distribution of more than 300,000 "Best Practices Guides" – with detailed instruction on the search and seizure of electronic evidence – to local, state and federal law enforcement officers. We have distributed more than 20,000 *Forward Edge* training CDs, which shares our expertise in cyber crime cases with state and local law enforcement. And, in partnership with the Federal Trade Commission, International Association of Chiefs of Police and the U.S. Postal Inspection Service, we have provided more than 25,000 Identity Crime Video/CD-ROMs which contain more than 50 investigative and victim-assistance resources for use by state and local law enforcement in combating identity crime, to every law enforcement agency in the country.

The Secret Service is typically able to move rapidly on investigations, and we are proactive in sharing case information with our partners. Representatives from the Secret Service, FBI and US Postal Inspection Service all responded to the arrest of a Ukrainian national who was deeply involved in cyber crime; primarily credit card fraud. At the time of his arrest, this suspect was in possession of technology which had not been seen previously by law enforcement. The Secret Service immediately drafted a Department of Homeland Security (DHS) Intelligence Bulletin on this new technology – called a dedicated data destruction device, or RASKAT. This bulletin was disseminated to all DHS Directorates, as well as Europol, Interpol and other U.S. law enforcement agencies. The Secret Service subsequently purchased one of these units in Russia, and forwarded it to the United States Computer Emergency Readiness Team (US-CERT) for examination and analysis. The results of these findings will be the subject of a future Intelligence Bulletin.

The Secret Service's expertise and success in the areas of critical infrastructure protection and cyber crimes has led to our being tasked with supporting a variety of initiatives as a bureau of DHS. An example of the Secret Service's proactive stance and involvement in critical infrastructure protection is the recent hosting of the DHS "Cyber Storm" exercise. The purpose of Cyber Storm – the largest cyber exercise ever initiated – was to test governmental communication mechanisms. The scenarios exercised during cyber storm centered on attacks on the national infrastructure and high level cyber crime. The majority of the law enforcement events and responses were handled by the Secret Service and the FBI. In addition to hosting this momentous exercise, the Secret Service turned to the Electronic Crimes Task Forces and was pleased with their performance.

Another important component in our investigative response to cyber crime and critical infrastructure protection is our Electronic Crimes Special Agent Program (ECSAP). This program is comprised of approximately 175 special agents who have received extensive training

in the forensic identification, preservation, and retrieval of electronically stored evidence. Special Agents entering the program receive specialized training in all areas of electronic crimes, with particular emphasis on computer intrusions and forensics. ECSAP agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence, including computers, personal data assistants, telecommunications devices, electronic organizers, scanners and other electronic paraphernalia. Furthermore, all Secret Service agents, including ECSAP agents, understand that not only are they criminal investigators but also that they are an important part of the preventive component of critical asset protection as they can provide important feedback to the public and industry regarding vulnerabilities that are discovered during an investigation.

In today's high tech criminal environment, the challenge to federal law enforcement and government is to identify existing repositories of expertise and provide a framework for inclusion and productive collaboration amongst the many government agencies and their respective industry and academic counterparts. The Secret Service is convinced that building trusted partnerships with the private sector and our Federal and local law enforcement partners, as well as continuing in our efforts to educate the public on how they can reduce the threat of data breaches and improve their system security, is the model for combating electronic crimes in the Information Age.

It should also be noted that although a large percentage of the private sector breaches to which the Secret Service provides investigative assistance and support are large data brokers, corporations or financial institutions, we do not differentiate based upon the size of the victim or the amount of potential loss. We are equally concerned with compromises being experienced by small companies or ISOs, and will respond with the appropriately trained personnel when notified of a suspected compromise. This is why we believe so strongly in a proactive educational platform as a preventative measure.

Mr. Chairman, that concludes my prepared statement, and I would be happy to answer any questions that you or other members of the subcommittee may have.

Testimony of
Steven M. Martinez
Assistant Deputy Director, Cyber Division
Federal Bureau of Investigation
Before the House Committee on Small Business
Regulatory Reform and Oversight Subcommittee
March 16, 2006

Good afternoon Chairman Akin, Ranking Member Bordallo, and members of the committee. I want to thank you for this opportunity to testify before you today about Small Business Cyber-Security Issues.

As retail business moves to the world of e-commerce, cyber crime will follow. In 2000 e-commerce accounted for 1% of all retail sales. Today it accounts for 2.4% of all sales. This upward trend will undoubtedly continue. Adding to this the revenue generated by non-retail Internet businesses, such as media and entertainment; e-commerce will soon dominate all commercial activity worldwide. The FBI is committed to investigating threats at all levels against this major force in our economy.

Small business forms a vital link in the overall security of the Internet. First, small business accounts for a significant portion of the retail business occurring on the Internet. Many online businesses and e-retailers are small businesses, many small businesses are customers of online businesses, and still other small businesses support the IT and Internet operations of large businesses and the government. Second, the integrity of Internet-connected small business systems has an impact on the security of the Internet as a whole.

The FBI has recognized that the best way to combat the growing threat of cyber crime is to

form a partnership with businesses and industries that rely on the Internet for their success. By teaming up with the private sector the FBI is able to find out what issues affect business and what problems are causing the most harm. This has allowed us to focus our efforts on the major problems affecting the Internet. Further, through our outreach and information-sharing initiatives we are able to share our experiences with the business community so that they can better protect and defend themselves against new and evolving cyber threats. The education of small businesses about the scope and nature of cyber threats is an important first step in protecting those businesses.

The FBI has two initiatives focused on building a partnership with business: The National Cyber-Forensics and Training Alliance (NCFTA) and InfraGard. The NCFTA is a first-of-its-kind public-private alliance located in Pittsburgh, PA. At the NCFTA members of law enforcement work side-by-side with representatives from business on addressing the latest and most significant cyber threats. Through this collaboration the FBI has been able to identify and prosecute some of the most serious cyber criminals including those who distribute computer viruses, operate large networks of compromised computers (known as botnets), and perpetrate fraud schemes such as phishing scams. The NCFTA is strategically located near Carnegie Mellon University's Computer Emergency and Response Team / Coordination Center (CERT/CC) and is also within driving distance of the FBI's Internet Crime Complaint Center (IC^3).

As an example on how we address cyber complaints, the NCFTA was recently contacted by a small bank in New Jersey. The bank was the victim of a phishing attack. In this type of attack the criminal creates a fake website that is identical to the real bank site and uses the fake site to steal credit card and other identity information from the bank's customers. With the victim bank to help them, the NCFTA traced the attack to its source and identified what measures they could take

to mitigate the effects of this attack. With the help of the NCFTA, the bank was able to send "cease and desist" letters to the Internet service providers hosting the fake sites in order to have the sites shut down.

InfraGard is an alliance between the FBI and the public whose mission is to prevent attacks, both physical and electronic, against critical infrastructure including, but not limited to banks, hospitals, telecommunications systems and the Internet. InfraGard has over 14,800 private sector members spread across 84 local chapters throughout the United States. These private sector partners represent the full spectrum of infrastructure experts in their local communities. FBI Agents assigned to each chapter bring meaningful news and information to the table such as threat alerts and warnings, vulnerabilities, investigative updates, overall threat assessments and case studies. The FBI's private sector partners, who own and operate some 85 percent of the nation's critical infrastructures, share expertise, strategies, and most importantly information and leads that help the FBI track down criminals and terrorists.

The IC^3 is a joint initiative between the FBI and the National White Collar Crime Center (NW3C). Located in West Virginia, a short distance from the NCFTA facility in Pittsburgh, the IC^3 serves as a clearing house for cyber crime incidents reported by both individuals and business. The IC^3 receives, on average, 25,000 reports of cyber crime incidents each month. By analyzing these complaints for commonalities and trends the IC^3 is able to develop cases that have a national impact. These cases are then referred to local, state, or federal law enforcement agencies for investigation.

As with the NCFTA, the IC^3 also focuses on partnerships with business as the most efficient and effective way to combat cyber crime. In 2002 the IC^3 began an initiative to help

online retailers combat fraud from re-shipping scams. The initiative known as REtailers and Law Enforcement Against Fraud (RELEAF) brought together teams of analysts at the IC^3 and e-commerce businesses to identify fraudulent online purchase which were being shipped by domestic re-shippers to destinations overseas. In one 30-day period, the RELEAF initiative resulted in 17 arrests, 14 controlled deliveries, the recovery of $340,000 in stolen merchandise, and the recovery of over $115,000 in counterfeit cashier's checks.

An important issue in combating cyber crime is education and awareness. This is even more important for small businesses that may not have the personnel or financial resources to secure their online systems to the same level as larger businesses and organizations. The NCFTA and InfraGard initiatives all have a significant awareness/education component to their collaborative efforts with business. In 2005 the FBI and United States Postal Inspection Service teamed up with several industry groups such as monster.com, Target, the Merchants Risk Council, and the Spamhaus Project, to create the LooksTooGoodToBeTrue.com web site. This website contains information for the lay person regarding various types of cyber crimes and means of online protection. The LooksTooGoodToBeTrue.com web site received over 3.1 million hits during its first week of operation alone.

In closing, the FBI is committed to investigate threats at all levels on the Internet. Director Robert S. Muller's vision in creating the Cyber Division, in fact demonstrates this commitment. The aggressive and creative strategy the FBI has employed by partnering with business and academia will create an environment focused on information sharing which will allow us to develop actionable intelligence in order to better address the ever growing Small Businesses Cyber-Security issues.

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Testimony of
Ari Schwartz
Deputy Director
Center for Democracy and Technology

Before

The House Committee on Small Business Subcommittee on Regulatory Reform and Oversight

March 16, 2006

Hearing on "The State of Small Business Security in the Cyber Economy"

Chairman Akin and Ranking Member Bordallo, thank you for holding this hearing on cyber security, an issue of growing concern for consumers and businesses alike. CDT is pleased to have the opportunity to participate.

CDT is a non-profit, public interest organization dedicated to preserving and promoting privacy, civil liberties and other democratic values on the Internet. CDT has been a widely recognized leader in the policy debate about the issues raised by spyware, phishing and related privacy threats to the Internet. As we have worked to build trust on the Internet, we have been required to become experts on the large and growing range of cyber-security threats facing Internet users. I'll briefly touch on how home of those threats affect small businesses, individuals and anyone who relies on the Internet as a tool for communication and commerce.

I. Growing Attacks Pose Threat to the Potential of the Internet

In the 15 years since the birth of the World Wide Web, the Internet has fundamentally altered the way we interact. It has created unprecedented opportunities for enhancing democracy and civil liberties worldwide as well as providing fertile new ground for international commerce.

The Internet levels the playing field for individual speakers and small businesses. It is a cheap and effective way to reach around the world. There are factors that make the Internet unique among communications tools, but its strength has always been its open, decentralized, and user controlled nature.

But that fundamental strength is also one of the Internet's greatest vulnerabilities. Just as networking and interconnectivity allow for unprecedented sharing of ideas, those factors also expose the medium to a virtually limitless source of new threats. The Internet today is being buffeted by unceasing torrent of viruses, spam e-mail, phishing scams and spyware.

Individually, these attacks are dangerous enough, but taken together they have begun to chip away at the trust Internet users have in the medium. This poses a grave threat to the Internet's continued growth. Recent studies have shown that viruses, spam, phishing and spyware have changed the way consumers and businesses use and view the Internet. A recent study by the Pew Internet & American Life Project found that 91% of Internet users say they have made at least one change in their online behavior to avoid unwanted software programs.[1] The National Cyber Security Alliance and AOL found that 24% of Americans believe that their home computer is "Not Very" or "Not At All" safe from hackers.[2]

Declining trust in the Internet is a major concern to the broader potential of the medium for two reasons. First, commerce on the Internet is dependant on mutual trust. For example, a recent survey by Consumer's Union has indicated that 25 percent have stopped making purchases online, and 29 percent of have cut back on online purchases because of concerns about identity theft.[3] Second, solutions suggested to solve many of the Internets ills would change the very nature of the Internet. For example, some have suggested charging per email sent to cut down on spam, phishing and email spread viruses. While such a change may cut down on some types of problem emails, it would also drastically change the nature of emails to the detriment of small business, who can have unlimited communications with their partners for a set price today. Such changes could also have dangerous consequences for anonymous and pseudonymous political speakers in repressive regimes who, under the current e-mail structure, are able to broadcast their message to audiences around the world at no cost and with minimal censorship.

To address these dangers, we must ensure both that our proposed solutions get to the root

---

[1] Susannah Fox, Spyware: The threat of unwanted software programs is changing the way people use the internet," Pew Internet and American Life, July 2005.
http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf
[2] AOL/NCSA Online Safety Study, December 2005
http://www.staysafeonline.info/pdf/safety_study_2005.pdf
[3] Consumer Reports "Do we trust the Internet?: Our poll finds that Web users are increasingly wary and demanding," October 2005. http://www.consumerreports.org/cro/personal-finance/the-latest-information-on-internet-user-trust-1005/overview.htm?resultPageIndex=1&resultIndex=10&searchTerm=identity-theft

of the problem, and that those solutions don't inadvertently harm the essential nature of the medium.

II. Financial Motivation for Attacks

To reach these goals we must understand the motivation and character of the threats. Although popular portrayals of Internet criminals continue to focus on young hackers vandalizing Web sites or launching denial of service attacks to gain notoriety among their peers, most of the real threats today are driven instead by financial gain.[4]

CDT has observed this evolution in our efforts to fight spyware. In 2004, we filed a complaint with the FTC against Seismic Entertainment, a company that was hijacking computers, getting paid by software distributors to install pop-up advertising programs and then attempting to sell its victims software to clean up the mess it created. The FTC filed a case and when discovery documents were released the next year, we found that the head of Seismic had known that exactly what he was up to. "I figured out a way to install a [self-executable software program] without any user interaction," he wrote to his partners in an email. "This is the time to make the $$$ while we can."[5]

Unfortunately, criminals with this attitude are finding new ways to attack consumers and businesses on the Internet all the time.

In particular, we have observed an increase in the following financially motivated attacks:

1. **Identity Theft** including:

- "Phishing" schemes in which 'spoofed' e-mails to lead consumers to counterfeit banking and e-commerce websites where they are prompted to divulge financial data such as credit card numbers, account usernames, passwords and social security numbers.

---

[4] Joris Evers, "Hacking for Dollars," CINet.com, July 6, 2005. http://news.com.com/Hacking+for+dollars/2100-7349_3-5772238.html

[5] Federal Trade Comm'n. Mem. in Support of Leave to Name Additional Def.'s. and File First Am. Compl., Att. A, Federal Trade Comm'n v. Seismic Entertainment Productions, Inc., et al, 04-377 (D. N.H.)

- "Keyloggers" and "password crackers" are software often used maliciously by attackers to surreptitiously track users' online activities and steal sensitive data directly.

2. **Corporate Espionage** using software designed to collect sensitive information. Such schemes are often funded by competitors.[6]

3. **Advertising software that provides popups** have been a consistent source of funding for cyber criminals. The adware companies pay distributors and individuals per installation. As documented above in the Seismic case, this provides an incentive to install by ay means necessary. It is also important to note that many adware companies receive ad revenue from legitimate Fortune 500 companies who place pop-up ads through ostensibly legitimate distributors.[7]

4. **Spam schemes** including those in which criminals hijack hundreds consumer and business computers and use them to send messages in a bid to avoid detection.[8]

5. **CyberExtortion**, such as that discussed in the Seismic case, where criminals hijack computers and then attempt to sell services to fix them or where corporate thieves steal information and hold it for ransom.

It is important to note for this committee that all of these attacks have a magnified impact on small businesses. Many small businesses suffer from attacks aimed at both consumers and businesses. Also, while large enterprises can afford spare capacity in the form of additional computers and servers, many small businesses don't have that luxury.

---

[6] One of law enforcement's biggest breaks in such a case came earlier this month — William Eazel "Husband and Wife Trojan Team Indicted," SC Magazine, March 7, 2006. http://www.scmagazine.com/uk/news/article/544861/husband-wife-trojan-team-indicted.

[7] CDT is releasing a report on this phenomenon today entitled "Where Does the Money Come From?: How Advertising Dollars Encourage Nuisance Adware and What Can be Done to Reverse the Trend." Please visit our Web site – http://www.cdt.org for more information.

[8] Dan Ilet, "Most Spam Generated by Botnets," ZDNet UK, September 22, 2004. http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm

When a computer goes down or is rendered unstable in a small business setting, the financial impact can be immediate and profound.

We are beginning to see more attacks that rely on multiple techniques, also known as blended threats that are uniquely targeted to a specific type of user. The New York Times recently reported that large gangs of criminals in Brazil and Russia are using virus-like techniques to install password crackers that only work on certain bank Web sites.[9] This story demonstrates not only the new skills of the criminals, but also the international nature of the threat. We have also seen an increase in techniques used to obscure nefarious programs. All of these developments make this type of threat much harder to defend against.

III. Conclusions

While the growing threats are cause for concern, it is important to note that there are reasons to be hopeful.

Computer security software, when utilized by consumers and business, has greatly improved protection. For example, the NCSA/AOL study found that 80 percent of consumers had some kind of spyware on their computers in October 2004. This number had dropped to 61 percent of consumers in December 2005.[10] Since we continue to see the number of threats rise,[11] this drop can only be explained by the growing quantity and quality of anti-spyware products.

Because of the changing nature of the threats, it is important that these programs continue to improve. In particular, computer security companies have done an excellent job finding problems and distributing information about whatever malicious program caused the problem, but they are only just beginning to look for programs that display signs of bad behaviors before those programs are known.

---

[9] Tom Zeller Jr., "Cyberthieves Silently Copy as You Type," New York Times, February 27, 2006, pA1.
[10] AOL/NCSA Online Safety Study, October 2004 http://www.staysafeonline.info/pdf/safety_study_v04.pdf and AOL/NCSA Online Safety Study, December 2005 http://www.staysafeonline.info/pdf/safety_study_2005.pdf
[11] Webroot Software, "State of Spyware Report 2005: The Year in Review," February 2006.

It is important that the knowledge gained by security companies be used in cooperation with law enforcement. CDT continues to bring cases and we have had many security companies join our efforts and offer assistance to law enforcement, but we will need greater cooperation to continue to keep up with the criminals.

Similarly, law enforcement must work better across borders. The biggest breaks in cases have come when law enforcement follows the money trails to identify networks of criminals. Sometimes this trail goes cold at the border because law enforcement does not have the tools to share information. CDT believes that this type of sharing can both protect civil liberties and help lead us to the real criminals

Finally, it is essential that we spend more time on where the money is coming from to motivate individuals to break the law for the fast infusion of funds. Who is paying the corporate spy? Do companies realize that they are advertising through spyware? What are the products advertised in spam emails? Answering these questions will not solve all cyber security problems, but it will cut off a significant flow of funds to many of the worst actors.

Testimony of Enrique T. Salem
Senior Vice President, Consumer Products and Solutions
Symantec Corporation

Before the
U.S. House Small Business Subcommittee on Regulatory Reform and Oversight

Hearing on the State of Small Business Security in a Cyber Economy

March 16, 2006

I would like to begin by thanking Chairman Akin and Ranking Member Bordallo for giving me the opportunity and privilege of testifying before the House Small Business Subcommittee on Regulatory Reform and Oversight at today's hearing on *the State of Small Business Security in a Cyber Economy*.

I am hopeful that my remarks will provide the Committee with a comprehensive overview of the U.S. small business cyber threat landscape. I also hope to provide some thoughtful insights on the many security challenges small business owners face in an economy growing more dependent on an Internet connected world. I look forward to responding to the Committee's questions following my remarks.

I come before you today representing Symantec Corporation, the global leader in providing information security solutions to help protect consumers and businesses by assuring the security, availability and integrity of their information. Headquartered in Cupertino, California, Symantec is the world's fourth largest software company with operations in more than 40 countries and over 17,000 employees.

As Senior Vice President for Consumer Products and Solutions, I am responsible for Symantec's worldwide consumer business including the small business marketplace. Prior to joining Symantec, I was president and CEO of Brightmail, the leading provider of anti-spam software so I'm especially familiar with the challenges small businesses face with spam. I also provided comments to Congress on legislative language recommendations for the CAN SPAM Act.

Last week Symantec released the findings of its ninth semi-annual Internet Security Threat Report, or ISTR, which is widely acknowledged to be the most comprehensive analysis of security activity for today's information economy. The Report includes an analysis of network based attacks including those on small businesses with a review of known threats, vulnerabilities, and highlights of malicious code and additional security risks. Symantec has provided this Report semi annually since 2002.

The ISTR is unique in that it is grounded principally on the expert analysis of real data gathered from one of the most comprehensive collections of Internet threat data in the world. We have over 24,000 sensors

monitoring network activity in more than 180 countries via Symantec DeepSight Threat Management System and Symantec Managed Security Services. In addition, malicious code data, spyware and adware reports are gathered from more than 120 million client, server, and gateway systems. Symantec's database of security vulnerabilities is one of the world's most comprehensive resources, covering more than 13,000 vulnerabilities affecting more than 30,000 technologies from more than 4,000 vendors. Finally, the Symantec Probe Network is a system of more than 2 million decoy accounts, which attracts e-mail messages from 20 different countries, allowing Symantec to gauge global spam and types of identity theft activity such as phising.

Symantec issues this free Report as a public service to educate consumers, businesses and government with the information they need to effectively protect and secure their computer systems now and in the future. The ISTR also offers security best practices for consumers and businesses to help them protect against current and emerging cyber crime threats.

Symantec's ISTR found that small businesses have consistently been in the top three most targeted groups for cyber attacks over the past year. In the first six months of 2005, small business was the second most targeted group for attacks. In the second half of 2005, small businesses were the third most popular targeted group behind financial services and education. This pattern demonstrates that small businesses are increasingly being targeted by attackers. Cyber criminals have found that small businesses are less likely to have a well established security infrastructure, making them more vulnerable to attacks.

While past attacks against small businesses were designed to destroy data, today's cyber crimes are increasingly designed to silently steal data for profit without doing noticeable damage that would alert a user to its presence. In the previous ISTR, Symantec cautioned that malicious code for profit was on the rise, and this trend continued during the second half of 2005. We can conclude from these findings that cyber crime represents today's greatest threat to consumers' digital lifestyle and to small businesses which primarily operate their activities online. I'd like to submit a copy of the Symantec's Internet Security Threat Report to the Record for today's hearing with the Chairman's permission.

In addition to the Internet Security Threat Report, Symantec sponsored the first comprehensive study of its kind analyzing the state of information security readiness in the U.S. small business market. The July 2005 study entitled, "Small Business Information Security Readiness," was conducted by the Small Business Technology Institute (SBTI), a non-profit, public benefit corporation whose goal is to foster the adoption of information technology among small businesses.

The SBTI study, which surveyed more than 1,000 small businesses with up to 100 employees, found conclusive evidence that information security is a high priority for small business owners, but also showed that this market represents a critical point of security exposure and vulnerability for the national economy.

The study findings reveal a lack of appreciation of the true economic impact of information security incidents and a lack of knowledge of cyber threats. Additionally, the study revealed a lack of forward planning and matching investment required to maintain the security necessary to protect small businesses as they deploy increasingly sophisticated information technology infrastructure and automate more of their business processes.

I'd like to submit a copy of this study for the hearing Record again with the permission of the Chairman. Some key findings from this study that signal the escalating information security risk to small businesses for the Committee to consider include:

- The accelerating adoption of networking and mobile computing infrastructures is driving greater security exposure for small businesses. Many small businesses lack sufficient security controls over even basic systems such as e-mail (18 percent are not secured) and wireless networks present a new area of concern (60 percent are not secured).

- While over 70 percent of small businesses consider information security a very high priority, they are not increasing their investment in protection to keep pace with the increasing number of threats. This is because small businesses demonstrate an alarmingly complacent, passive attitude to information security.

- We found that over 80 percent of small businesses surveyed are overly confident in their existing digital security measures. Only a small number (30 percent) have increased spending on information security solutions in the past year and less than half (41 percent) allocate a specific budget for these solutions.

- This overconfidence has resulted in a majority of small businesses (56 percent) having experienced at least one security incident in the past year, citing computer viruses, spyware and other malware as the main cause.

- Small businesses manifest are overwhelmingly reactive in purchase decisions when it comes to Internet security with 35 percent of small businesses increasing spending on security products

only after they were compromised or attacked by suffering a data loss or corruption.

- Another key finding is that over 74 percent of small businesses perform no information security planning whatsoever. Small businesses demonstrate limited awareness of information security issues, best practices and have a poor understanding of the economic consequences of related incidents. SBTI's analysis concludes that this lack of knowledge and awareness is inhibiting the adoption of adequate information security policies and solutions.

It is difficult to quantify the economic impact of cyber crime but according to the FBI's 2005 Cyber Crime Survey cyber crime costs about $67 billion to U.S. firms over the last year. Additionally, the Federal Trade Commission found that identity theft costs businesses $48 billion annually, and last year cost consumers $680 million in losses.

But more damaging than the loss of money is the loss of trust and confidence by consumers in the Internet economy which so many of our nation's small businesses depend upon. We can't risk losing the public's confidence in doing online transactions with small businesses so it's essential that they have the right resources to protect themselves. Symantec continues to play an instrumental role in protecting small businesses through the security solutions we offer and our education and awareness efforts.

I would like to conclude my testimony by saying that small businesses are just as likely to experience information security threats and risks as large enterprises, so it's pertinent they have the right resources to protect their critical assets. Symantec continues to play an instrumental role in protecting small businesses through the security solutions we offer and our education and awareness efforts.

For example, Symantec is a major sponsor of the National Cyber Security Alliance (NCSA), a non-profit organization established to educate consumers, small businesses and educational organizations how to stay safe online. The NCSA website, staysafeonline.org, has many useful awareness tools and resources for small businesses and partners with the Department of Homeland Security, FTC, Small Business Administration, NIST, many companies and other non-profits on several initiatives, including the small business training workshops lead by NIST.

In addition to its sponsorship of the NCSA, Symantec has created several tools, including educational books and CD-ROMs, which address the unique needs of small businesses. We have copies of these materials available at today's hearing. Symantec has also developed a wide range of security and data protection solutions that specifically address the needs of small businesses.

The information security knowledge gap can only be closed through the joint efforts of government agencies, information security vendors and non-profit organizations. We must focus on increasing cyber security awareness, education and enabling small businesses to properly assess their true level of risk and encourage them to take the necessary preventative and corrective measures.

Symantec looks forward to continuing to work in partnership with organizations in the private sector and Congress to conduct research and create tools that lead the way in providing U.S. small businesses with the right resources they need and deserve to truly be secure and prosper in today's high-tech global economy.

Thank you again, Chairman Akin, for allowing me the opportunity to testify before the distinguished members of the House Small Business Subcommittee on Regulatory Reform and Oversight.

TESTIMONY BEFORE THE

COMMITTEE ON SMALL BUSINESS, SUBCOMMITTEE ON REGULATORY REFORM AND OVERSIGHT

U.S. HOUSE OF REPRESENTATIVES

March 16, 2006

By Dr. Burton S. Kaliski, Jr.

Introduction

Chairman Akin, Ranking Member Bordallo and other distinguished members of the Subcommittee, my name is Burt Kaliski. At RSA Security, I serve as Chair of the Chief Technology Office and as Vice President of Research. I am also Chief Scientist of RSA Laboratories, the research center of the company.

The letters "RSA" stand for the initials of three MIT professors who in 1977, under federally-funded research, invented a public-key encryption algorithm that is now in use worldwide. With that heritage of research, RSA Security leads the way in strong user authentication and encryption, bringing trust to millions of user identities and the transactions that they perform. RSA Security's portfolio of award-winning identity & access management solutions helps businesses of all sizes to establish who's who online – and what they can do.

At RSA Laboratories, we conduct applied research that addresses emerging online threats as well as evolving IT security challenges. Some of our current research topics include:

- **Privacy and security for Radio Frequency Identification (RFID) systems.** Like the Internet did, RFID promises to transform the way we do business. But also like the Internet, RFID introduces new threats for business and consumers to grapple with. Our researchers are developing new technologies that focus on building security into RFID from the start, so that we will all reap the benefits of the technology without so many of the risks to privacy and security that are now being discussed and debated around the world. This is an important issue for businesses and organizations of all sizes in both the private and public sector.

- **Knowledge-based authentication.** Many Web sites are asking their users to answer personal questions – such as a mother's maiden name or place of birth. These often are not as secure as organizations would like. Researchers at RSA Laboratories are studying how to choose questions that are easier to remember, and harder to guess. As we move beyond passwords because of challenges such as identity theft, this type of user authentication becomes more and more important.

My staff and I are also very active in information security standards initiatives, working to develop standards in cryptology, authentication and other areas of IT security. In addition to participating in several industry standards bodies, RSA Laboratories has played an important leadership role in developing the Public-Key Cryptography Standards (PKCS) for encryption and the more recent One-Time Password Specifications (OTPS) for strong authentication.

As a member of the IT community, I currently serve on the board of trustees for the Massachusetts Technology Leadership Council (http://www.masstlc.org), and I am a member of the IEEE Computer Society and the International Association for Cryptologic Research.

I am honored to be in front of the Subcommittee to address today's hearing topic: "The State of Small Business Security in a Cyber Economy."

Given the IT security challenges that businesses and consumers face online – and the significant impact that the Internet continues to have on our economy and our daily lives – this is a critical topic to address. More and more businesses of all sizes hold sensitive and personally identifiable information on consumers and it is vital in today's online environment to be able to protect that information, no matter how big or small your organization is. While the Internet is an incredible enabler of business-to-business and business-to-consumer transactions, cyber-criminals are exploiting vulnerabilities like never before to steal information and financial assets.

I think that it's worth referencing a recent story in a major domestic newspaper that highlighted what we have been seeing in the information security industry over the last year or so: as large companies put more protections in place, cyber-criminals are going after smaller businesses. On major analyst, who was quoted in the story, says that "... crooks are going after 'less technically savvy' companies."

The bottom line is that no organization or individual, whether you are a large corporation, a government agency, or a small business or consumer, is exempt from this threat. Cyber criminals are in it to make serious money and they will go where information and assets are vulnerable and available for exploitation.

Small and Medium-Sized Businesses Face Significant Information Security Challenges

At the recent industry-wide RSA Conference (www.rsaconference.com) in San Jose, the Director of the FBI, Robert Mueller, said that while the Internet has become a global growth engine for business, it has also become "a global target for cyber-criminals." Information technology has become a "force-multiplier for criminals," he added.

Director Mueller is exactly right. The Internet is being utilized more and more as a tool to enable cyber-crime. The days of a teenage hacker launching a computer virus just because he/she could, can be remembered – while not fondly – at least as a relatively

simple type of online nemesis; now, however, this is somewhat of a distant memory. The cyber-criminal of 2006 is often a sophisticated, skilled and well-organized thief who is constantly updating and improving upon his/her techniques and aiming attacks at IT systems that have vulnerabilities which can be quickly exploited for profit. Yes, cyber-crime has become big business – a way for nefarious individuals to exploit relatively easy prey.

In 1989, I first joined what was then called "RSA Data Security" – a very small business itself at the time. To describe the technical aspects of how cyber security threats have changed during those years would take much more time than we have today. The reality is that cyber security challenges are constantly evolving: day to day, week to week, month to month. Even companies such as ours that focus completely on IT security are constantly challenged to stay on top of, and ahead of, the constantly-changing threat environment in cyberspace.

You will no doubt hear from my Symantec colleague today how the nature of overall cyber threats have changed from last year to this year. In my view, these threats fall into basically two broad categories, and each warrants a particular focus from small businesses and their consumers/customers.

- First, **outside attacks**. A small business will be increasingly under threat from organized attackers outside the business – and often outside the country – who seek to break into the small business's IT systems – or, still worse, steal information from the small business's customers through phishing attacks and various forms of "malware." Big business is under attack too, of course, but small businesses may not have as many resources and as much experience to apply against such attacks, and so will become more attractive targets.

- Second, **inside attacks**. A small business will also increasingly be under threat from organized attackers inside the business. These "insiders" are not so much the employees, who in a small business may often be well enough known to one another to minimize any particular threat. Rather, the threat may come from the various service providers and "partners" who often will be granted access to corporate data in order for the small business to fulfill its mission. For instance, a small business will often need to rely on a "trusted third party" to run its Web site – or even to administer its IT systems. But what if the third party can't be trusted?

  Also, a small business will often open its systems to partners through whom it is attempting to expand its business opportunity, and these also introduce potential threats. Again, big business faces similar challenges, but they also often have developed policies and procedures to deal with them, and they can usually compartmentalize their IT systems to limit exposure – thus, the whole business is not on the line for most major corporations. The same cannot be said for many small and medium-sized businesses.

As I mentioned earlier in my testimony, organizations of all shapes and sizes now hold sensitive information on individuals. Under current law, the Federal Trade Commission (FTC) has held businesses accountable if they don't protect personally identifiable information. In the past, the FTC has taken action against businesses under the "deceptive practice" clause; now they are pursuing actions based on an "unfair practice" e.g. if you hold sensitive information on individuals then you had better have processes in place that will protect that data.

What this translates into is that small and medium-sized businesses are more exposed not just to threats in cyberspace but to the liabilities and negative publicity that comes with it. As the U.S. Congress and States consider new laws and regulatory regimes in this area, businesses of all sizes have to take legal exposures seriously. Also, it is important for legislators and regulators to also think about what impact new laws will have on small and medium-sized businesses.

What Can Small and Medium-Sized Businesses Do?

Let's face it, small businesses are just that: organizations that are relatively small in size and that don't have big budgets or substantial human resources to dedicate to protecting IT systems. They generally don't have an information security department. (They may not even have an IT department!)

But small businesses are the backbone of our national and global economy and in the Internet age, this community is more vulnerable than ever to cyber-crime. It's quite a dilemma for small businesses: in order to enable more growth via online transactions, you expose yourself to more threats to your business and could even end up going out of business if you don't have adequate IT security.

What is an adequate level of information security for small and medium sized businesses? As is the case for larger organizations, security should be commensurate with the value of the data or resource being protected, and the level of risk. Just as you don't shred every piece of paper you discard, you don't have to encrypt every file of data – but you had better shred, or encrypt, the more sensitive materials. Similarly, just as you don't put a lock on every door or filing cabinet in an office building, you don't have to authenticate access to every system with the same high level of security – but you had better restrict access to the more sensitive areas, especially when there's an elevated threat level or set of substantial risks to your business.

While there is certainly no technology silver bullet, there are baseline IT security practices and processes that every small business should consider after assessing their risk and exposure to online threats. Anti-virus and intrusion prevention systems are essential in the online world. Software needs to be kept up-to-date with the latest security patches. Information should be classified according to its sensitivity: Even something as simple as "public," "company confidential," and "personnel" can be a step forward. And identity and data protection needs to be managed, based on policies appropriate for those classifications.

Let me expand upon the last point a little. Once an organization has labeled its data according to sensitivity, it can restrict access to the data based on permissions. The small business owner might have access to all the data, but service providers and external partners might only have access to selected data. If the data is also encrypted, then access to the keys required to decrypt the data can also be restricted based on permission. For instance, a vendor that offers data backup and recovery services to the company might only receive the encrypted data, but not the decryption keys.

In order to realize these forms of data protection, an organization needs to be able to authenticate the users that are coming into its system: to verify that someone's claim of a particular identity or permission is correct. Traditionally, such verification has been based simply on a password. Passwords still offer reasonable security in some situations, but when there are higher risks – such as sensitive information on individuals that needs protection - it has become very clear across multiple industries that something more is needed.

Small businesses are expert at making the most of what they have. In the case of user authentication, they actually have many more resources at their disposal than they may be aware of. Although a password itself is only one "factor" in determining whether a claimed user is authentic, many other factors are available for an organization that is looking for them.

One such factor is a "risk score." A risk score is an indication of whether a particular transaction by a claimed user looks out of the ordinary for that particular user – in terms of the type of transaction, time of day, network location, and so on. A transaction can be compared against those previously reported as fraudulent to see whether there is increased evidence of risk. Based on a risk score, an organization can decide to ask the user for more information, such as the answers to pre-determined personal questions, or perhaps even contact the user directly. But if the risk score is low enough, the password – plus the assurance of lower risk – can be adequate to grant the requested access to the user. This is part of an overall "adaptive" approach to security where, rather than forcing the same solution onto everyone and all situations, the appropriate combination of technologies and processes can be selected that responds to the risk and fits the specific situation.

Because fraudsters often threaten multiple organizations, businesses are organizing "fraud networks" to share information about reported fraud. Small businesses in particular can benefit from these networks because they serve as an "early warning system". The small business does not have to rely on its own, limited transaction history to determine what might be risky in the future, but instead can draw from the multiplied experience of large organizations and numerous other small businesses alike.

Various security devices are also available to small businesses seeking to provide their employees and consumers with an additional physical factor for authentication. Industry offers a growing range of implementation options. A small business can provide these

devices to its users directly. For example, RSA Security has an appliance specifically targeted to the small business market that lets an organization of 250 or fewer users easily deploy our market-leading RSA SecurID® two-factor authentication solution. Alternatively, organizations can rely on devices the users already have – for instance their mobile phones, or security devices they've obtained already through their account relationships with other businesses.

Finally, there is the issue of awareness and education – making information available to small businesses and consumers to educate them on cyber security threats and easy-to-understand and implement steps that will help improve their cyber security posture. There are a number of helpful websites where small businesses and consumers can go to learn more about basic steps and information security best practices, including: the National Cyber Security Alliance's StaySafeOnline campaign at www.staysafeonline.org – which has targeted information for both small businesses and consumers; the FTC's Onguard Online site for consumers at www.onguardonline.gov; and for alerts on the latest cyber security threats go to the U.S. Department of Homeland Security's U.S. CERT site at www.us-cert.gov.

The IT Industry Can Play a Key Role in Protecting Information Too

As I mentioned earlier in my testimony today, I have been with RSA Security since the late 1980s. Believe me; a lot has changed in the information security and broader IT industry during that period of time! The IT industry is prioritizing information security more than ever. One very public display of that heightened focus and prioritization is highlighted every February when the RSA Conference is held in northern California.

The RSA Conference was founded 15 years ago; when it was first established by my company, you basically had around 50 technologists and cryptologists discussing the technical details of the Digital Signature Standard. The Conference has evolved into the largest industry-wide forum on information security issues in the world, with over 14,000 individuals attending annually and with IT industry leaders such as Bill Gates, John Chambers, and Scott McNealy speaking there. This is certainly a testament to how the security industry has grown over the years, but it's also proof that the major platform vendors recognize the critical importance of IT security to their businesses, their customers, and to consumers. What's more, the attendee mix at the RSA Conference has dramatically changed over the years. Yes, we still have technologists and cryptologists who participate annually, but now just about every stakeholder you can imagine attends the Conference, including small- and medium-sized businesses, and yes, we even get an occasional Member of Congress to participate!

One of the highlights of the RSA Conference is the annual Cryptographers' Panel. Prof. Ronald Rivest of MIT (the "R" in RSA), Prof. Adi Shamir of the Weizmann Institute (the "S"), Dr. Whitfield Diffie of Sun Microsystems, and Prof. Martin Hellman of Stanford University - four of the pioneers of modern cryptography - were all members of the panel this year. I served as the moderator for a typically fascinating 45-minute discussion of recent events in the field.

Prof. Shamir announced his latest results on the security of RFID systems: A simple power analysis attack on a certain implementation of RFID tags by which a modified RFID reader could deactivate a tag without authorization. This work is significant because of the growing importance of RFID tags in supply-chain applications, which - again - has an impact on businesses of all sizes. Imagine the effect on future commerce of physical goods if a rogue RFID reader – perhaps in the form of a future mobile phone – could deactivate all the tags in a store or warehouse. We know from experience with Internet security that what the research community is concerned about at one time – such as the lack of authentication of e-mail – may well become a practical threat years later. On the other hand, systems that are designed with security built-in avoid many of these threats – this is a lesson that we have learned the hard way from the Internet.

The panelists also spoke about the importance of usability. Good security that's easy to use is better than great security that's not – because great security that's not usable won't be used at all. The original design of public-key cryptography, as the panel discussed, assumed that each user was associated with a personal encryption key. That has turned out to be very hard to realize in practice because most users can't remember encryption keys, and no users can do complex cryptography with those keys without the assistance of a computer. So, in practice, the user has to trust a computer to do cryptography with the user's personal key. The user's computer becomes the weak link: Attackers can undermine security just by compromising the user interface in order to get passwords. In fact, designers can undermine security just by making the user interface for security features so complicated that users don't use it.

Any feature can be a lot more usable if it's built into mainstream software and services, rather than added on later. Consider the relative ease of connecting to the Internet today, for example, compared to five or 10 years ago. Each year at the RSA Conference, more and more security vendors are taking the point of view that security needs to be built-in: from the hardware to the operating system to the network. At RSA Conference 2006, it was encouraging to see the emphasis that IT industry leaders placed on building-in security, and the ownership their companies were taking for their part of improving security. To the extent that key software and service providers power small businesses' IT infrastructures, this is a good sign of things to come.

Security is indeed getting easier to use, and I would like to highlight a few other recent developments in the IT security industry that provide encouragement in this direction.

First, vendors are finding ways to make security more usable across the industry as a whole – not just for one company at a time. After all, consumers don't interact with just a single company; they have a complex, dynamic set of interactions with multiple companies all over the Internet. Imagine what it would be like if every merchant accepted only its own charge cards. Company-specific security solutions are much like this. Even if the security interfaces look the same on different Web sites (and hopefully they would to reduce user confusion), the security still might not interoperate from one site to another. As examples:

- Many sites ask users to answer security questions, but they don't necessarily ask the same questions, nor do they share the answers with one another. As a result, users have to remember the answers to many questions, possibly asked slightly differently on separate sites, and perhaps even answered slightly differently in each case.

- Some sites also provide users with security devices (e.g., smart cards, biometric readers, one-time password devices) as an additional authentication factor. But they don't necessarily share the same device with other sites. As a result, users may have to carry multiple security devices. To some extent, this is reasonable; users have different keys to unlock doors at work and at home, for example. But by analogy with charge cards, it would be better to have the same "key" for all one's personal interactions.

As more organizations, including small businesses, add security features, the ability to share those security features with other organizations will become increasingly important. "Token sharing" – the re-use of security devices at different sites – is being architected into security designs, such as work by the Liberty Alliance's Strong Authentication Experts Group (www.projectliberty.org), or the Financial Services Technology Consortium's Better Mutual Authentication Program (www.fstc.org). Services that enable effective token sharing are offered by RSA Security and other vendors. "Federation" is another approach for sharing security features, by centralizing the full authentication process – user name, password and possibly security device – at an identity provider service. Both approaches offer a path toward better industry-wide security that will also help small businesses.

Second, vendors are finding ways to make usable security features more widely available. It is remarkable to consider that more than a billion people now carry computers with them wherever they go in the form of mobile phones. Perhaps the vision of every user being associated with a cryptographic key will be realized, where the key is contained in a device that the user already carries for more everyday purposes. Rather than adding a security device to a system, vendors are looking for ways to build security into the devices that are already in the system, like the mobile phones.

Users carry other computing devices as well – memory sticks, media players, even watches. Any of these can be a "container" for cryptographic keys. Multiple vendors again are working on ways to fulfill the potential of these everyday containers to provide enhanced security for online systems. As an example, RSA Security recently announced that it is working with several device manufacturers to enable their consumer devices – which will be available in the millions – to be employed as additional authentication factors in online systems (potentially including the "token sharing" option above).

Third, it used to be that you basically needed to be a "crypto engineer" to write software that encrypted your data and managed the encryption keys. Today, policy-based approaches are available where you just say "here's the kind of data I have, please

encrypt it." You can even use predefined policies for how each kind of data should be protected.

Fourth, the advent of security appliances – application servers that come with security software preinstalled – bodes well for small and medium-sized businesses. No longer do they need to buy extra computers and install software in order to have the security they need; they can just plug a security appliance into the network (if the security features aren't already built into the other servers they have). As I mentioned earlier in my testimony, RSA Security recently started offering a security appliance to enable our small and medium-sized business customers to implement two-factor user authentication more easily. Interestingly, we found that larger organizations who learned about the appliance also wanted one, so that they could more easily extend their own security infrastructure. This was a good example of the SMB market taking the lead in helping to shape the marketplace.

Finally, IT vendors are working on improvements to the user interface itself. Browser vendors recently agreed on a better way to present information about the name and authenticity of a Web site. There have also been improvements to interfaces for warning a user when a Web site does not seem trustworthy. Ultimately, vendors may arrive at a better way for the user to enter passwords and other personal information – an interface that can be trusted to represent an authentic site, and employ the provided information only for the purpose of authenticating to that site – not like the interfaces today that can potentially be under the control of a rogue application or site. Small and medium-sized businesses have a particular good perspective to bring on the user interface side of things, because the whole business is so closely connected to its users.

Based on these efforts by security vendors, in the near future, a small business will have many options for strengthening security in a usable manner, more than ever before. The small business will be able to rely on a common, trustworthy interface to the user; the user will be able to employ a familiar device of his or her choice in order to authenticate to the small business (or, no additional device at all); and the authentication will be interoperable across different sites. Although a small business could in principle roll out its own interface software and its own devices for its own purposes, this doesn't scale well if every small business took the same approach. Instead, some businesses will promote some of these components, and others will just leverage the infrastructure that's being built, all for the common good.

Strengthening the Public-Private Partnership for Better IT Security

Much has been said about the importance of a public-private partnership to secure cyberspace over the years. The *National Strategy to Secure Cyberspace* that was issued by the President in 2003 established an excellent foundation for this partnership to succeed. In fact the strategy highlighted the role of small businesses and consumers in national efforts to improve cyber security: "Home users and small businesses can help the Nation secure cyberspace by securing their own connections to it." Another recommendation in the Strategy emphasized the importance of national awareness

programs: "DHS, working in coordination with appropriate federal, state, and local entities and private sector organizations, will facilitate a comprehensive awareness campaign, including audience-specific awareness materials, expansion of the StaySafeOnline campaign, and development of awards programs for those in industry making significant contributions to security."

RSA Security has been an active participant in public-private sector efforts to increase cyber security awareness nationally for a number of years. Since 2003, RSA Security has been a supporter of the National Cyber Security Alliance (www.staysafeonline.org) and this public-private partnership's national cyber security awareness campaign. Organizations such as the U.S. Department of Homeland Security (DHS), the U.S. Federal Trade Commission (FTC), EDUCAUSE (www.educause.edu), and INFRAGARD (www.infragard.net) have been active participants and supporters of this initiative, as have several corporations including strong support from AOL, Bell South, Cisco Systems, McAfee, Microsoft, and Symantec. The primary purpose of this organization is to be a resource for raising cyber security awareness to the consumer, small business, and education audiences. The site provides information on cyber security threats and best practices for protecting against those threats that consumers and small businesses in particular can understand and easily implement. Both the DHS and private corporations such as ours have donated time and money in support of this initiative. We encourage other organizations – both in the public and private sector – to do the same.

The StaySafeOnline awareness programs have reached millions of users over the last year, but more work needs to be done, particularly with the small business community. As a participant in this partnership, RSA Security would specifically encourage the Small Business Administration (SBA) to become more involved in this public-private initiative, given their role in working with the small business community. We would also recommend that private sector organizations with direct links to small businesses – such as Chambers of Commerce in America's cities and states – also become more directly engaged in this important effort.

The National Institute of Standards and Technology (NIST) plays an incredibly important role in development standards for the U.S. federal government. Over the years, NIST has been instrumental, through its work with private industry, in fostering the development of cryptology standards. NIST also has provided expertise and training to the small business community via NCSA programs as part of the Stay Safe Online initiative in various cities throughout the U.S. as well as via the Internet. In short, the work of NIST is pivotal for the private sector as well as the government and we encourage their ongoing participation in public-private partnerships such as NCSA.

Overall, government has a role to play to make the partnership more successful in the years ahead and that role should not just be limited to education and awareness programs. Federally-funded cyber security research and development is also very important. Much of our industry would not exist without federally-funded research – in fact, the Internet would not exist without the early R&D investments made by the U.S. government. In February 2005, the President's Information Technology Advisory Committee (PITAC)

issued a report entitled *Cyber Security: A Crisis of Prioritization*, which included several recommendations, including: "Increase Federal support for fundamental research in civilian cyber security by $90 million annually at the NSF and by substantial amounts at agencies such as DARPA and DHS to support work in the 10 high-priority areas identified by the PITAC." While the Bush Administration responded in the FY2007 federal budget with substantial increases in funding to the NSF/National Science Foundation, this is only one step forward. The U.S. Congress should approve that budget request and also provide the necessary oversight that will ensure that many of the PITAC's recommendations are implemented.

Finally, there is the area of breach notification legislation. Nearly two-dozen states have passed new laws that require breach notification if sensitive information on individuals is exposed; most of these laws are modeled after California's SB 1386, the first breach notification law in the country. As Congress considers federal legislation in this space, we would encourage the U.S. House of Representatives and U.S. Senate to develop a national breach notification framework that will protect consumers and also establish a national baseline that businesses of all sizes can comply with. The reality is that many small and medium-sized businesses also hold personally identifiable information on individuals and will likely have to comply with any new federal law. Therefore, to incentivize and reward businesses that do adopt industry best practices such as encryption – which renders the breached information unreadable by unauthorized parties - we encourage the inclusion of a safe harbor provision for encrypted information. That position has been endorsed by IT industry organizations such as the Business Software Alliance (www.bsa.org) and Cyber Security Industry Alliance (www.csialliance.org), and all 23 state laws that are currently on the books have some form of encryption exemption language. An encryption safe harbor will prevent over-notification of consumers and will reduce the burden on small and medium-sized businesses that are implementing industry best practices such as encrypting sensitive information.

Conclusions

1. Just because you're a small or medium-sized business doesn't mean they – the cyber-criminals – aren't out to get you, too; your resourcefulness also makes you an attractive target.
2. But just because you're a small or medium-sized business doesn't mean you can't do anything about the threat. You don't need to be a big business with an IT security department to have better IT security for your business.

There's a great deal that these businesses can already do – and more that they can do in the future.

- Security is being built in to many new software and systems in a way that's easier to use and administer, so it's more automatic.
- One size doesn't fit all: An adaptive approach to security can fit the requirements of your business as well.

- Tools for encrypting data and managing encryption keys are available that are easier to use – you don't need a degree in cryptography.
- Network-based security services are being set up that can manage part or all of your identity management and authentication – in a way that can interoperate with what other businesses are doing. But if you prefer to manage part or all of the security yourself, there are a growing number of security appliances available that can just be "plugged in" to your network – no software to install or additional computers to buy.
- Fraud networks also have tremendous potential in helping small and medium-sized businesses to identify potentially fraudulent transactions, leveraging the knowledge of larger organizations and many other key businesses as well.

With all these tools being made available, businesses should have high expectations for the IT security industry to help fulfill the potential for safer online commerce.

RSA Security was once a small business. Even today, and in particular at our research center, RSA Laboratories, we maintain that entrepreneurial perspective. We look forward to working together with small and medium-sized businesses toward a stronger and more secure online economy.

Testimony of

The Computing Technology Industry Association (CompTIA)

Roger J. Cochetti

Group Director-U.S. Public Policy

Before the House Small Business Committee

Subcommittee on Regulatory Reform and Oversight

On the

"The State of Small Business Security in a Cyber Economy"

Thursday, March 16, 2006

Good afternoon, Chairman Akin, Ranking Member Bordallo, and distinguished members of the Subcommittee. My name is Roger Cochetti. I am Group Director for U.S. Public Policy of the Computing Technology Industry Association (CompTIA) and I am here today on behalf of our 20,000 member companies.

Mr. Chairman, I want to thank you and the Members of your Subcommittee for holding this important hearing on the state of small business security in the cyber economy. We believe that your efforts to focus public attention on the factors that affect cyber security and small business will help American small businesses more ably address, thwart and remediate cyber threats.

As this Subcommittee knows, small business is the backbone of the American economy. Some 23 million small businesses employ over half of the private sector workforce and are a vital source of the entrepreneurship, creativity and innovation that keeps our

economy globally competitive. They are responsible for over half of our GDP, and their share is growing. Moreover, Americans depend upon small business for virtually every aspect of their daily lives. So, as a nation, we are dependent upon the health of the small business sector.

Today, nearly all American small businesses are dependent upon information technology (IT) and most are increasingly dependent upon the Internet. Failures in the IT infrastructure, or in the Internet, threaten the viability of American small business; and their vulnerability to cyber threats is America's vulnerability.

In the United States and elsewhere, the IT needs of small businesses are mainly addressed by an important segment of computer industry called Value-Added Resellers, or VARs. These small system integrators set up and maintain computer systems and networks for small businesses.* An estimated 32,000 American VARs sell some $43 billion dollars worth of computer hardware, software and services; mostly to small companies. This means that over one third of the computer hardware sold in the U.S. today is sold by VARs, again mostly to small businesses. VARs are, therefore, the front line in the American defense against cyber security threats.

Mr. Chairman, the Computing Technology Industry Association represents the business interests of the information IT industry. For 24 years, CompTIA has provided research, networking and partnering opportunities to its 20,000 mostly American member companies. While we represent nearly every major computer hardware manufacturer and software publisher, nearly 75% of our membership is comprised of American VARs. Therefore, we particularly appreciate the opportunity to testify before this Subcommittee because for our VAR members, cyber security is not a theoretical concern: it is what they must build into the services that they provide to their clients.

VARs service just about every small business in America. Your dentist, travel agent, local retailer, or dry cleaner contracts with their local VAR to install, maintain and service their IT needs. For example, the local area network in your

dentist's office is most likely not installed or maintained by the dentist. This is true for other small businesses as well. This work is almost certainly performed by a local VAR.

In addition to representing the interests of the small IT companies called VARs, through our headquarters in Chicago, and our public policy offices in Washington, Brussels, Hong Kong and Sao Paulo, CompTIA works to provide global policy leadership for the IT industry, and nowhere are we more active than in the area of cyber security policy. For most people in the computer industry, however, CompTIA is well known for the non-policy-related services that it provides to advance industry growth, standards, professional certifications, industry education and business solutions.

In order to most efficiently serve the industry and our members, CompTIA has developed specialized initiatives and programs dedicated to major areas within the IT industry. Some of the services that we offer that are relevant to this hearing include:

- Educating VARs and Other Small IT Companies on Cyber Security
  With support from Congressional and State officials and many of our larger member companies, last year we launched a series of educational outreach programs for VARs on the problems and issues raised by cyber security. These new programs aim to reach out to the thousands of small IT businesses that make up the bulk of our membership and help them better understand what the Federal government and large corporations are doing in this area and explain how they can get more involved.

- Professional Certifications for IT Workers
  CompTIA offers 12, vendor-neutral professional certifications that test and validate a variety of baseline technical and professional IT skills. CompTIA A+, Network+, CDIA, i-Net+, Server+, Linux+, IT Project+, e-Biz+, CTT+, HTI+ (Home Technology Integrator), RFID+, and Security+ certifications provide credibility, recognition of achievement and quality assurance for employers and employees alike.

Most importantly for this hearing, we have developed the industry standard for validating an IT professional's abilities in the area of cyber security called the **Security+** professional certification. It is one of our most popular professional certifications with 23,357 IT professionals certified worldwide since 2002.

- Public Policy

  CompTIA's public policy program addresses the policy and regulatory concerns of the IT community at the federal, state and international levels. We do this by educating our members about developments in the policy process and encouraging them to get more engaged and by advocating policy solutions that make sense for the nation and for the IT industry.

  Most importantly for this hearing, we have been an active partner with the White House, the Department of Homeland Security, the Federal Trade Commission and the Small Business Administration in seeking policy solutions to the issues posed by cyber security threats in general and cyber security threats to small business in particular.

- Helping the IT Industry Understand Privacy Regulations

  CompTIA provides a formal structure and method for service executives to communicate and resolve industry issues such as standard terminology warranties and how to address new and challenging issues that IT companies collectively face.

  Most importantly for this hearing, we have launched a series of parallel efforts to help the industry understand the complexities and implications for IT integrators of such recent Federal regulations in the area of consumer privacy as those resulting from Graham, Leach Bliley and the Health Insurance Portability and Accountability Act (HIPAA.) Threats to consumer privacy under these laws and regulations very often result from threats to cyber security. This is as true for small business as it is for large companies.

Further background information on many of our activities can be found on our website at www.comptia.org.

Given the importance of small business to the U.S. economy and the importance of VARs as the IT enablers of small business, it is somewhat surprising that cyber security concerns of the small business segment of our economy has not received greater attention. At the federal level, several important but modest efforts have been launched aimed at educating small business about the basic issues in cyber security; and we are pleased to say that we have been involved in nearly all of them. As I will explain later, we believe that much more needs to be done, however.

The State of Small Business Cyber Security:

Beginning in 2002, CompTIA has commissioned annual IT security benchmarking studies entitled "Committing to Security – A CompTIA Analysis of IT Security and the Workforce." The study is a cross-sector analysis of the state of IT security as well as an examination of the root cause of most IT security breaches.

The benchmark study surveys professionals across a myriad of industries to answer pressing questions about the dynamic landscape of IT security. The study provides insights into IT security practices and highlights security challenges confronted by organizations of varying sizes and sectors. Approximately 65% of the respondents are small businesses with annual revenues below $10 million.

To briefly summarize, CompTIA's Cyber Security Study reveals that the IT security landscape has changed significantly, along with the rapidly changing technology used across industries. The benefits of Internet communications and commerce in the global marketplace have also been exploited with malicious intent. This is evident in the surge of Internet viruses, worms and phishing (e-mails containing URLS that direct users to fraudulent websites) in the past year. Though security software has become increasingly more advanced in its ability to detect security threats to networks, applications and

operating systems, hackers are often sophisticated enough to reverse-engineer patches and launch counter-offensives to vulnerable systems within 48 hours. Even the most sophisticated security software solution, which can provide 24 hours of security detection and assessment, cannot replace fully the need for IT security awareness and training in the workplace.

In past years, viruses have infected millions of small business users across the globe. For example, a pervasive worm known as Sasser infected more than 500,000 computers last year; a very large proportion of them used by small businesses. Within a month's time, the worm had mutated several times and a malicious hybrid called Korgo appeared, causing havoc by stealing personal information as it passed from system to system.

Most non-technology based organizations are slower to adopt security software and slower to implement security awareness training to end-users. Security decision-makers without proper training often underestimate the cost and threat of security breaches to their organization. Other decision-makers, including small business managers, lack the empirical support to rationalize the needed investment for IT security.

Overall, CompTIA's Cyber Security Study reveals that there is a large discrepancy between the IT security that organizations say they need and the level of education and prevention occurring within these organizations. In 2005, the forth annual CompTIA Study on IT Security and the Workforce found that nearly 40% of organizations experienced a major IT security breach – defined as one that causes real harm, results in the loss of confidential information or interrupts business – within the last six months. The number of serious IT security breaches remained consistent between 2002, 2003 and 2004.

Human error, either alone or in combination with a technical malfunction, was blamed for four out of every five IT security breaches (approximately 80%), the CompTIA study found. That figure is not statistically different from previous years. Security assurance continues to depend on human actions and knowledge as much, if not more so, than it does on technological advances.

The CompTIA Study found that organizations, including small businesses, may not be taking all the steps necessary to protect themselves. Among areas where organizations are coming up short in their preparedness:

- More than half the organizations surveyed (53%) do not have written IT security policies. This figure is unchanged from previous years.

- One-half of the organizations have no plans to implement security awareness training for their employees outside the IT department, nor have they considered it.

- About two-thirds of organizations (63%) have no plans to hire IT security personnel in the next year.

- Training and certification requirements are still uncommon for both current employees and new hires. Just 27% of organizations require IT security training; and 12 % require certification.

Yet overwhelmingly (89%), organizations believe that major security breaches have been reduced as a result of IT security training and certification. The positive effect of training and certification is most often described in terms of improved potential risk identification, increased awareness, improved security measures and an ability to respond more rapidly to problems. The lack of written IT security policies present at more than half the responding organizations fosters gaps in security knowledge, especially among end-users. Even at organizations with written security policies in place, enforcement of security policies continues to be a problem.

To be truly effective in preventing and combating security threats, small businesses need to take further steps by spreading security awareness and knowledge from a select group of IT staff to larger portions of their employee base.

Specific to small business, the CompTIA survey found that:

- Small businesses are less likely to report a security breach;
- 72% of small businesses with under 50 employees do not have a written IT security policy in place;
- 49% of small businesses with under 250 employees do not have a written IT security policy in place;
- The most commonly mentioned reason for the human errors (52%) that led to security breaches is the failure of staff to follow security procedures.

Based on our studies, it is very clear that more needs to be done to raise cyber security education and training within the small business community. It is also clear to anyone who understands how small businesses operate in the United States that VARs must play the central role in any effort to reach out to small business in this area. What is most needed is a government industry partnership that takes advantage of the unique access and perspective of the thousands of VARs who IT-enable small business in the U.S.

Mr. Chairman, let me emphasize at this point that the most effective solution to nearly all cyber security threats – to small businesses or to any other IT user – do not rely on new federal or other regulations. The nature of the Internet in particular, as a global network of networks that is dynamic and rapidly changing, is such that government regulations will be of limited impact.

Much more effective in dealing with threats like cyber security are technology tools, industry best practices and consumer and business education; backed up by strong law enforcement. The key role that government agencies can and should play – aside from arresting and prosecuting criminals – is to work with industry on education, technology tools, and best practices.

We look forward to working with this Subcommittee and the relevant agencies in such a cooperative effort.

Federal Agency Outreach to the Small Business Community:

Let me begin by stating that we believe important work is being done to improve the state of cyber security in small businesses. Still, more can and should be done.

The Department of Homeland Security (DHS) has begun an outreach effort through the "Stay Safe Online" campaign. An important feature of this campaign is that DHS has wisely chosen to partner with the private sector in this effort. While "Stay Safe Online" is a modest program, it does reflect an important first step in the direction of increasing the awareness and education of small business and, potentially, the VARs who enable them.

The Federal Trade Commission, through its OnGuard Online program, of which we are proud to say we are a sponsor, its printed materials, the willingness of its staff to reach out to the small business community and its other educational programs on cyber security, provides educational tools that are useful to both consumers and small business. These modest efforts provide important resources that support every other effort to improve small business awareness and education on cyber security.

We are very pleased to report that the Small Business Administration is participating in CompTIA's regional cyber security outreach program. CompTIA has recently sponsored a cyber security conference for VARs in Santa Clara, California and will be holding four more events in 2006: all specifically aimed at the small IT businesses. We are delighted that the Washington Metropolitan Area District Office of the U.S. Small Business Administration has enthusiastically agreed to participate in our events to help us in educating this centrally important industry. Obviously, much more than CompTIA's score of local conferences for VARs needs to be done and we look forward to working with the SBA in designing more and better programs and enlisting their support for them.

We also recognize that the National Institute of Standards and Technology (NIST) has an important technical advisory role in cyber security across the board. However, we are not

aware of any outreach or educational programs sponsored by the Institute that involves VARs in their outreach.

Conclusion

U.S. small business sector is vital to the overall health of the American economy and our national security. This segment of the American economy is almost entirely dependent for its IT enablement on small system integrators who specialize in serving the needs of small businesses called Value Added Resellers, or VARs, of which there are tens of thousands across the country. These VARs hold the key to reach small business and helping them improve their cyber security awareness and preparation.

Small businesses are particularly vulnerable to cyber attacks and should be more diligent in developing adequate cyber security practices. The evidence suggests that they are neither trained nor prepared for cyber threats as much as they should be.

To improve this situation, the federal government and industry, particularly VARs, need to work together to reach out to small business and help small business better understand the nature of the threat and the practical things that they can do to address it.

A number of federal agencies have gotten off to a good, although quite modest, start in reaching out. Much more now needs to be done, however.

---

* According to the Small Business Administration (NAICS code 541519), "an Information Technology Value Added Reseller provides a total solution to information technology acquisitions by providing multi-vendor hardware and software along with significant services. Significant value added services consist of, but are not limited to, configuration consulting and design, systems

integration, installation of multi-vendor computer equipment, customization of hardware or software, training, product technical support, maintenance, and end user support".

Statement of Howard A. Schmidt

President & CEO

R & H Security Consulting LLC

Testimony before the House Committee on Small Business, Subcommittee on Regulatory Reform and Oversight

Hearing on the State of Security on Small Businesses in a Cyber Economy

March 16th, 2006

Chairman Akin, Ranking Member Bordallo, distinguished Members of the Committee: My name is Howard A. Schmidt and I am President & CEO of R & H Security Consulting LLC. Over the past 20 years I have served as a Computer Crime Investigator, with the Chandler Arizona Police Department, led the computer exploitation team for the FBI at the National Drug Intelligence Center as well as the Director of Computer Crime and Information Warfare at Air Force Office Special Investigations. I have also been the Chief Security Officer for the Microsoft Corporation and Chief Information Security Officer and Chief Security Strategist for eBay Inc. In the aftermath of 9/11, I was appointed by President Bush as the Vice Chairman of the President's Critical Infrastructure Protection Board and Special Advisor for Cyber Security. I also serve as an Adjunct Professor with Georgia Tech, GT Information Security Center and as an Adjunct Senior Fellow, with Carnegie Mellon University, CyLab.

I want to thank you for the opportunity to share with the Committee my perspective on the State of Small Business Security in a Cyber Economy, an issue on which this Committee's leadership to raise public awareness of the great benefits and potential operating in the cyber economy. Your willingness to work closely with the private and public sector makes your contribution to this issue even more valuable.

During my previous testimony before House Committees, I have discussed the implications of cyber security on our day to day lives and the protection of critical infrastructure. Today, I would like to spend a few minutes talking about the

improvements that have been made in the past few years which give the small and medium businesses (SMBs) much more effective, lower costs and easier to use tools to protect themselves and their customers online. My distinguished colleagues on both panels have done a superb job explaining the threats that face the SMBs today and why the challenges threaten more than just our privacy and protection of personal information, but also affect our confidence to work online with them. I will speak briefly as to the progress that market forces and the private sector have made in the past year. It has been proven time and time again, the tremendous value that results when the public and private sectors work together to protect innovation as well as to improve end user protection.

I would like to categorize the "Cyber" capabilities into three groups:

1) SMBs where their IT systems are also their computer systems that are also their main personal computers. This is especially true in the case of "Mom and Pop" business where all of their online business is run from one computer system.

2) SMBs where they have dedicated computer systems for their business operations and a small IT staff to maintain their systems, but do not have the luxury as do large enterprises of large staff that have specific expertise in IT Security.

3) SMBs that contract with an IT service provider that run the systems for multiple customers from" virtual servers." This gives the SMB a turn key operation the permits them to focus on their core business competency and allow someone else to manage the

IT requirements.

With these categories in mind, the level of success hinges on four things; technology, awareness and training, information sharing and law enforcement investigations.

A. Technologies:

To deal with this, industry, using market forces, have responded rapidly to deal with technologies needed to make security easier, more comprehensive and more robust.

1. Software developers have invested heavily in tools and processes to reduce the number and severity of security flaws in commercial software during the software development life cycle, often cited as the most commonly exploited aspect of computer attacks by criminals. There still needs to be more work done, but more recent applications have less security bugs and when they are found a more comprehensive cycle of repair is now in place.

2. In order to identify the existence of potential security vulnerabilities, there are now "web based" vulnerability assessment services that do not require building an internal vulnerability capability, making identification easier and cheaper.

3. Automatic updating of anti-virus applications, spy-ware and spam ware is now common place. Many service providers now provide free/low cost anti-virus services for their users. Operating system vendors also now have auto updating features as well as other security companies provide robust patching services reducing the complexities of dealing with patching computers.

4. Technology now exists through browser "toolbars" that turn Green, Yellow or Red, depending on the level of trust of particular web sites, giving their customers more confidence in shopping online. New filters block fraud, malware and "phishing" emails from even getting in the customer's inbox providing better trust in doing business with SMBs.

5. There is also new technology that provides and "all in one" DSL/Cable modem, Wireless Router, Anti-Virus, Virtual Private Network (VPN), Anti-Phishing, Anti-Spam, Anti-Spyware and content filtering all built into one gateway device that is professionally managed giving the same protections that large enterprises have at significantly lower costs.

6. Two factor authentication and Identity management tools are become more widely accepted. The impact of fraud and doing

business with unknown customers has always had level of risk. Now many companies are deploying two factor authentications that gives a higher level of confidence of who you are doing with, reduce the likely one will become a victim of ID Theft and credit card misuse.

7. Encryption technologies are now easier to use, more reliable, less resource intensive and overall more widely accepted. The ability to encrypt connections, data at rest, credit card numbers and other personally identifiable information (PII) can now be a part of any size business with relative ease.

B. Awareness and Training

1. There is a real need for SMBs to understand that threats against IT systems are not just directed against large companies and large enterprises. There is a real need to provide the SMBs with a clear understanding that criminal activity is often directed at them as well. Knowing that you are a potential target is important to understand how to keep from becoming a victim.

2. The Treasury Department has released a DVD on called "Identity Theft; Outsmarting the Crooks" that is available to a wide audience

including SMBs. The FTC, USPS, USSS, Army CID as well as other private sectors groups worked to create this DVD. Information can be found at: http://www.ustreas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml

3. The FTC has long been a leader in providing awareness and continues to lead in this role. In addition to the multiple efforts that they partner with other public and private entities, they have created a web site in concert with the Department of Commerce, Department of Homeland Security, USPS and the SEC. This web site provides a wealth of information that is vital to understanding cyber security and helps SMBs understand the threats that they and their customers face. http://onguardonline.gov/index.html

4. The National Cyber Security Alliance, formed in 2003 is a private-public partnership has a dedicated section to help SMBs learn about Cyber Security, Data recovery and reporting of cyber crimes. This information can be found at: http://www.staysafeonline.org/basics/small_business.html .

5. The Multi State ISAC, under the leadership of Will Pelgrin, from Governor Pataki's office, has worked with the states to provide the

awareness and training so states can pass this information on to their businesses and consumers in their jurisdictions. http://www.cscic.state.ny.us/msisac/ncsa/oct05/index.htm

6. The US-CERT, with the Department of Homeland Security provide free resources that allow businesses of all sizes receive alerts and best practices free of charge. http://www.us-cert.gov/

7. There National Cyber Security Partnership, http://www.cyberpartnership.org/ led by the US Chamber of Commerce, Technet, Business Software alliance and the Information Technology Association of America (ITAA) formed this partnership, in a true private-public partnership, created task forces to provide awareness to SMBs. http://www.cyberpartnership.org/init-aware.html

8. The Industry Security Alliance created a SMB "Common Sense Guide" to Cyber Security. This has been distributed through many organizations including the US Cert, Ready.gov, the US Chamber of Commerce as well as a number of other web sites. http://www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm http://www.ready.gov/business/st3-improvecyber.html

C. Information Sharing:

1. A number companies, even competitors, are working closely together to identify new threats, share information with each other and publish updates to deal with new threats faster than ever in the past.

2. The Infragard program, developed by the FBI, brings businesses of all sizes together with each other and law enforcement officers to share information and best practices. http://www.infragard.net/

3. The US Secret Service has created Electronic Crimes Task Forces, (ECFT) to bring private businesses of all sizes together for the purpose of information sharing and coordination of cyber crime/security issues.

4. Many of the same efforts listed in the Awareness and Training Section also have information sharing projects that are open to SMBs to participate in.

D. Law Enforcement Efforts

1. As with many other issues harming society, technology, education and information sharing are not 100% effective in solving problems.

To that end, the need to have penalties and well trained, equipped and staffed law enforcement personnel to enforce those penalties are essential. While online safety continues to improve day-by-day, hour-by-hour the work of the law enforcement community is vital to help us better protect SMBs by holding the criminals accountable and creating a deterrence in the process.

2. The very nature of cyber crimes makes them a challenge to smaller law enforcement agencies. The training to investigate and prosecute these cases needs to be supported at all levels of government.

3. In addition to the cyber crime reporting structure that the FTC has in place, the FBI with the National White Collar Crime Center, (NWCCC) operates the internet crimes complaint center. http://www.ic3.gov/ which takes reports, provides analysis of the activity then sends this information to state and local law enforcement agencies around the country. The IC3 also has a number of alliances with private and public organizations to better serve SMBs and consumers. http://www.ic3.gov/alliances.aspx . Below are examples of some of the alliances:

BUSINESS SOFTWARE ALLIANCE (BSA)

DIRECT MARKETING ASSOCIATION (DMA)

EBAY/PAYPAL

FEDERAL TRADE COMMISSION (FTC)

FINANCIAL SERVICES INDUSTRY

- Financial Institution Fraud Unit (FIFU)
- Financial Services Roundtable (FSR)

MERCHANT RISK COUNCIL (MRC)

MICROSOFT

NATIONAL CYBER-FORENSICS & TRAINING ALLIANCE (NCFTA)

NIGERIAN ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC)

REPORTING ECONOMIC CRIME ONLINE (RECOL)

- National White Collar Crime Center of Canada (NW4C)

UNITED STATES POSTAL INSPECTION SERVICE (USPIS)

There are some areas where there can be additional assistance by government and industry. With all of the information that is available online, much of it is still not reaching a large part of the SMB community as it relies on SMBs "pulling" this information off of the various web sites. Some large companies hold seminars for SMBs and ISVs and partners on cyber security but there are a lot of SMBs that are just not getting the word. One recommendation is to have a formal program where the SBA, FTC, Departments of Commerce and Treasury with DHS enhance their work with

organizations like the US Chamber of Commerce to reach out to local chambers of commerce and increase the access to resources to local SMBs. There are currently plans being made on many fronts to conduct such events and should be funded and supported.

On the law enforcement front, the SBA with its partners could work with the various crime prevention organizations at state and local levels to develop the cyber version of a "business security survey" This could be a valuable tool to local businesses to increase awareness, provide better processes and inform them on reporting procedures if something should happen.

In closing, we have made great progress since the President released the National Strategy to Secure Cyber Space in February 2003. In that document, the importance of the Small Businesses was clearly referred to a number of times and it is recognized that we all have to secure our own part of cyberspace and that the SMBs are an important part of that.

I again would like to thank the Committee for your continued leadership and attention to the benefits that SMBs receive from the internet and the use of IT and for extending the invitation for me to appear before you to share my experiences with you today and as in the future as this process evolves. Cyber security has always and always will employed using a "layered defense" perspective. By working with this body, technology companies, law enforcement agencies, and other government leaders, I believe we can continue to reduce the impact that bad actors have on our online

experience and we can continue to strengthen national security, public safety, and economic wellness of SMBs. We can be more secure while still providing for a rich and robust online experience for us all.

I look forward to any questions that you may have.

2006 Malware Survey

Dates: March 7-13, 2006
Respondents: 286 business owners

1. What type of business do you operate?

Manufacturing	26%
Retail	11%
Professional Services	49%
Finance/Insurance	4%
Construction/Real Estate	10%

2. How many full-time personnel are currently employed by your business, not including yourself?

Zero	12%
1-5	38%
6-19	28%
20-49	15%
50-99	5%
100-499	2%
500 or more	0%

3. Do you employ a dedicated IT person to maintain your office computers and IT infrastructure?

Yes	20%
No, I outsource it to a subcontractor	39%
No, I do all the work myself	41%

4. Have you ever lost business because of computer systems damaged or degraded by malware?

Yes	42%
No	58%

5. In 2005, what are the costs to your business attributable to malware, including repairs and damaged equipment?

Less than $100	38%
$101-$999	29%
$1,000-$4,999	24%
$5,000-$9,999	5%
$10,000 or more	4%

6. In 2005, how much forgone revenue did your business suffer because of malware?

Less than $100	52%
$101-$999	13%
$1,000-$4,999	19%
$5,000-$9,999	6%
$10,000 or more	10%

7. Has malware on your system ever caused you to lose customer information?

Yes	24%
No	53%
I have no way of knowing	23%

8. Do you conduct business via the Internet?

Yes	82%
No	18%