

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. MCHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
MARSHA BLACKBURN, TENNESSEE
PATRICK J. TIBERI, OHIO
KATHERINE HARRIS, FLORIDA

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

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

CONGRESSMAN ADAM PUTNAM, CHAIRMAN



OVERSIGHT HEARING STATEMENT BY ADAM PUTNAM, CHAIRMAN

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

Wednesday, September 22, 2004

2:45 p.m.

Room 2154, Rayburn House Office Building

OPENING STATEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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