CYBERSECURITY: WHAT THE FEDERAL GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

&

SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

January 8, 2016

Serial No. 114–56

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
20–826PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
F. JAMES SENSENBRENNER, JR., Wisconsin
DANA ROHRABACHER, California
RANDY NEUGEBAUER, Texas
MICHAEL T. McCAUL, Texas
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
BILL JOHNSON, Ohio
JOHN R. MOOLENAAR, Michigan
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BRUCE WESTERMAN, Arkansas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DRAIN LAHOOD, Illinois

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
DONNA F. EDWARDS, Maryland
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
KATHERINE M. CLARK, Massachusetts
DONALD S. BEYER, JR., Virginia
ED PERLMUTTER, Colorado
PAUL TONKO, New York
MARK TAKANO, California
BILL FOSTER, Illinois

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
MICHAEL T. MCCAUL, Texas
RANDY HULTGREN, Illinois
JOHN R. MOOLENAAR, Michigan
BRUCE WESTERMAN, Arkansas
GARY PALMER, Alabama
RALPH LEE ABRAHAM, Louisiana
DRAIN LAHOOD, Illinois
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
KATHERINE M. CLARK, Massachusetts
PAUL TONKO, New York
SUZANNE BONAMICI, Oregon
ERIC SWALWELL, California
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON OVERSIGHT

HON. BARRY LOUDERMILK, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
BILL JOHNSON, Ohio
DRAIN LAHOOD, Illinois
LAMAR S. SMITH, Texas

DON BEYER, Virginia
ALAN GRAYSON, Florida
ZOE LOFGREN, California
EDDIE BERNICE JOHNSON, Texas

CONTENTS

January 8, 2016

Opening Statements

Witnesses:

Appendix I: Answers to Post-Hearing Questions

Appendix II: Additional Material for the Record

CYBERSECURITY: WHAT THE FEDERAL GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR

FRIDAY, JANUARY 8, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY &
SUBCOMMITTEE ON OVERSIGHT,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 9:04 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Barbara Comstock [Chairwoman of the Subcommittee on Research and Technology] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 Rayburn House Office Building
Washington, DC 20515-6301
(202) 225-6371
www.science.house.gov

Subcommittees on Research and Technology and Oversight

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Friday, January 8, 2016
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

Witnesses

Mr. John B. Wood, Chief Executive Officer and Chairman, Telos Corporation

Dr. Martin Casado, Senior Vice President and General Manager, Networking and Security Business Unit, VMWare

Mr. Ken Schneider, Vice President of Technology Strategy, Symantec Corporation

Mr. Larry Clinton, President and Chief Executive Officer, Internet Security Alliance

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEES ON RESEARCH & TECHNOLOGY AND OVERSIGHT

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Friday, January 8, 2016
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

Purpose

On Friday, January 8, 2016, the Research & Technology and Oversight Subcommittees will hold a joint hearing to discuss various industry best practices relative to cybersecurity, share lessons learned from the private sector, inform on how innovative private sector security practices can be applied to government agencies, particularly in the wake of data breaches at the Office of Personnel Management (OPM), address the effectiveness of voluntary federal standards for cybersecurity, and discuss implementation of new cyber information sharing legislation. The Science, Space, and Technology Committee previously held a hearing on July 8, 2015 titled, *Is the OPM Data Breach the Tip of the Iceberg?* [1] The Committee's jurisdiction includes the National Institute of Standards and Technology (NIST), which develops cybersecurity standards and guidelines,[2] the Department of Homeland Security's Science and Technology Directorate (DHS S&T) and research and development related to cybersecurity at the National Science Foundation (NSF).

Witnesses

- **Mr. John B. Wood**, Chief Executive Officer and Chairman, Telos Corporation
- **Dr. Martin Casado**, Senior Vice President and General Manager, Networking and Security Business Unit, VMWare
- **Mr. Ken Schneider**, Vice President of Technology Strategy, Symantec Corporation
- **Mr. Larry Clinton**, President and Chief Executive Officer, Internet Security Alliance

Background

On June 4, 2015, OPM announced that it had identified a cyber-breach affecting personnel data for approximately 4 million current and former federal employees, including

[1] Hearing information available at: http://science.house.gov/hearing/subcommittee-research-and-technology-and-subcommittee-oversight-hearing-opm-data-breach-tip.

[2] As authorized by the Federal Information Security Management Act (FISMA) of 2002, enacted as Title III of the E-Government Act (Public Law 107-347) in December 2002, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf. NIST's responsibilities for cybersecurity were last updated in the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) available at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf, and Federal Information Security Modernization Act (P.L. 113-283) available at: http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf.

personally identifiable information (PII).[3] Later that month, OPM reported a separate cyber incident targeting its databases housing background investigation records, and announced on July 9th that an investigation concluded that the information of an additional 19.7 million individuals that applied for a background investigation had been stolen. The combined breaches are estimated to have compromised the sensitive information of 21.5 million individuals.[4]

On November 10, 2015, the OPM Office of Inspector General (OIG) released a FY 2015 audit report for the agency that continued to find an "overall lack of compliance that seems to permeate the agency's IT security program."[5] The audit found that the OPM has up to 23 systems that have not been subject to a thorough security controls assessment. The report states: "Combined with the inadequacy and non-compliance of OPM's continuous monitoring program, we are very concerned that the agency's systems will not be protected against another attack."[6]

The OPM breaches highlight the growing challenges of cybersecurity for both the public and private sector, as the number of cyber threats to both has grown exponentially in recent years. According to the U.S. Government Accountability Office (GAO), the number of information security incidents reported by federal agencies to US-CERT (the U.S. Computer Emergency Readiness Team, part of the Department of Homeland Security) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014 – an increase of over 1000 percent.[7]

A 2014 survey of private companies found that the number of detected incidents rose to 42.8 million, a 48% increase over 2013. The survey also found that the total financial losses attributed to security compromises increased 34% over 2013.[8] The impact to individual Americans grows too, as an estimated 12.7 million Americans experienced some sort of financial identity theft in 2014, costing $16 billion in financial losses.[9] In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, J.P. Morgan-Chase, Sony Pictures, and Anthem Health Insurance were only a few of the many publicly disclosed breaches.[10] The data breach of Anthem alone exposed the social security numbers of nearly 80 million Americans.

[3] OPM Press Release, "OPM to Notify Employees of Cybersecurity Incident," June 4, 2015. Available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident.

[4] OPM Press Release, "OPM Announces Steps to Protect Federal Workers and Others from Cyber Threats," July 9, 2015. Available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats.

[5] OPM FISMA FY 2015 Audit Report. Available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

[6] Ibid.

[7] *Actions Needed to Address Challenges Facing Federal Systems*, GAO-15-573T, April 22, 2015. Available at: http://www.gao.gov/products/GAO-15-573T.

[8] The Global State of Information Security Survey 2015. Available at: http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

[9] Herb Weisbaum, "Nearly 13 Million Americans Victimized by ID Thieves in 2014," NBCNEWS, March 3, 2015. Available at: http://www.nbcnews.com/business/consumer/nearly-13-million-americans-victimized-id-thieves-2014-n316266.

[10] 2014: A Year of Mega Breaches, Ponemon Institute, 1, (January 2015). Available at: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf.

Federal Cybersecurity Laws and Regulations

The federal role in cybersecurity involves both security for federal systems and assisting in protecting nonfederal systems. More than 50 federal statutes address various aspects of cybersecurity. These include:

Federal Information Security Management Act

The cybersecurity of federal systems is governed by the Federal Information Security Management Act, which was last updated by the Federal Information Security Modernization Act (P.L. 113-283) in December 2014. FISMA created a security framework for federal information systems, with an emphasis on risk management, and gave specific responsibilities to the Office of Management and Budget (OMB), National Institutes of Standards and Technology (NIST), and the heads, chief information officers (CIOs), chief information security officers (CISOs), and inspectors general (IGs) of federal agencies.[11]

FISMA makes OMB responsible for overseeing federal information-security policy, evaluating agency programs, and promulgating cybersecurity standards developed by NIST. Each agency must designate an information-security officer, with responsibilities including agency-wide programs, policies, and procedures, training of security and other personnel, processes for remedial action to address deficiencies, and procedures for handling security incidents and ensuring continuity of operations. Agencies must also develop performance plans, conduct independent annual evaluations of their cybersecurity programs and practices, and provide annual reports on compliance and effectiveness to Congress. FISMA requirements also apply to contractors who run information systems on behalf of an agency.[12]

Cybersecurity Enhancement Act of 2014

In December 2014, the *Cybersecurity Enhancement Act of 2014* (P.L. 113-274) passed the House and Senate and was signed into law. The law strengthens the efforts of NSF and NIST in the areas of cybersecurity technical standards and cybersecurity awareness, education, and workforce development. P.L. 113-274 coordinates research and related activities conducted across federal agencies to better address evolving cyber threats.

In December 2015, pursuant to Section 502 of the law, NIST developed and transmitted to Congress a plan ensuring federal coordination of international technical standards related to information system security. The plan "lays out the objectives and recommendations for enhancing the U.S. government's coordination and participation in the development and use of international standards for cybersecurity. The plan outlines four U.S. government strategic objectives for the development and use of international standards for cybersecurity: enhancing national and economic security and public safety; ensuring standards and assessment tools for

[11] *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, GAO-12-137, October 2011, http://www.gao.gov/new.items/d12137.pdf.
[12] *Cybersecurity: FISMA Reform*, CRS Insights, December 15, 2014.

the U.S. government are technically sound; facilitating international trade; and promoting innovation and competitiveness."[13]

Cybersecurity Act of 2015

In December 2015, the Consolidated Appropriations Act (P.L. 114-57) included the *Cybersecurity Act of 2015*. The new law encourages private companies to voluntarily share information about cyber threats with each other as well as the federal government. The Act directs the federal government to create a process for sharing both classified and unclassified cyber threat indicators and defensive measures with the private sector, as well as information relating to certain cybersecurity threats and best practices. Firms that participate in the information sharing will receive some liability protection.[14]

Executive Order 13636 on Improving Critical Infrastructure and Framework for Improving Critical Infrastructure Cybersecurity

In February 2013, President Obama issued an executive order (EO) on cybersecurity for critical infrastructure.[15] Among other provisions, the EO encouraged information sharing between public and private sectors and directed NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST was instructed to work with industry to identify existing voluntary consensus standards and industry best practices to incorporate into the framework.

In February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) in response to the EO. NIST worked in collaboration with industry stakeholders to establish a three-pronged framework that includes a Core, Profile, and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."[16]

P.L. 113-274 called for GAO to review aspects of the Framework, and in December 2015, GAO issued a report titled, "Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework." The report determines "the extent to which (1) NIST facilitated the development of voluntary cybersecurity standards and procedures and (2) federal agencies promoted these standards and procedures."[17]

[13] Letter from Dr. Willie E. May, NIST Director, to Chairman Lamar Smith, December 21, 2015.

[14] "President Obama Signs Cybersecurity Act of 2015 to Encourage Cybersecurity Information Sharing," National Law Review. Available at: http://www.natlawreview.com/article/president-obama-signs-cybersecurity-act-2015-to-encourage-cybersecurity-information.

[15] White House Press Release, "Executive Order – Improving Critical Infrastructure Cybersecurity," February 12, 2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[16] "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[17] *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152, December 17, 2015. Available at: http://www.gao.gov/products/GAO-16-152.

Chairwoman COMSTOCK. The Subcommittees on Research and Technology and Oversight will come to order.

Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

Good morning. Welcome to today's hearing titled "Cybersecurity: What the federal government Can Learn from the Private Sector."

In front of you are packets containing the written testimony, biographies, and Truth in Testimony disclosures for today's witnesses.

I now recognize myself for five minutes for an opening statement.

Today's hearing continues this Committee's commitment to find solutions for one of the great challenges of the 21st Century: cybersecurity. This is the second hearing we have held on cybersecurity since the news over the summer that the Office of Personnel Management was the target of two massive data breaches, exposing the sensitive information of over 21.5 million Americans, including many of my constituents. The OPM breach highlighted the growing challenge of preventing and responding to cyber threats for both the public and private sectors.

In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, and Anthem Health Insurance were only a few of the many publicly disclosed breaches. The data breach of Anthem alone exposed the Social Security numbers of 80 million Americans.

The time has come for every manager and every employee in both government and private organizations to make cybersecurity a top priority in their daily work, and for leaders to be held accountable for negligent failures to protect information. The American public and shareholders are demanding it.

When criminal hackers gained access to some 40 million Target customer credit cards, the CEO and the CIO were fired, in the private sector. Although the OPM Director resigned in the wake of the OPM breaches, I am still not satisfied that the responsible parties have been held accountable for the failure of the agency to address known security vulnerabilities.

The most recent IG audit found that OPM still has 23 systems that have not been subject to a thorough security controls assessment. OPM does not even have a complete inventory of servers, databases and network devices in their system.

Just this week I met with newly appointed Senior Cyber and Information Technology Advisor Clifton Triplett and the OMB Senior Advisor on Cyber and National Security.

I look forward to working with my colleagues and all federal agencies to ensure we are protecting the identities of our employees, applicants, and their families.

The cyber criminals, hacktivists, and state-sponsored cyber terrorists are getting more creative and bolder in their attacks. The private sector has been at the forefront of dealing with these threats for some time, as both the target of many of these attacks and as the leaders in developing the technology and workforce necessary to counter cyber threats.

Visa, which is in my district, is preparing to open a new Cyber Fusion Center in my district just this week. This state-of-the-art cyber facility brings together nearly 100 highly trained security professionals into one high-tech campus, and provides for collaboration both internally and with payments and with partners enabling information sharing, rapid response, et cetera. I am privileged to have a number of companies who are very much on the forefront in this area in my district, and we have a number of those witnesses here today, and I look forward to hearing from our witnesses, who are all innovative thinkers from the private sector.

I hope we can take the lessons we learn from you today, and help apply them towards protecting our federal information systems and the sensitive and valuable information they contain. We clearly must work together and be able to be more agile and adaptive to the ongoing threats that we know with the multiplication of information in our all of our systems which is just going to exponentially increase over the coming years. This will be a permanent employment area for all of you, I'm sure.

[The prepared statement of Chairwoman Comstock follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Research and Technology Subcommittee Chairwoman Barbara Comstock (R-Va.)

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Chairwoman Comstock: Today's hearing continues this Committee's commitment to find solutions for one of the great challenges of the 21st Century – cybersecurity.

This is the second hearing we have held on cybersecurity since the news over the summer that the Office of Personnel Management (OPM) was the target of two massive data breaches – exposing the sensitive information of over 21.5 million Americans, including many of my constituents.

The OPM breach highlighted the growing challenge of preventing and responding to cyber threats for both the public and private sectors.

In 2014 and 2015, cyber-attacks on Target, eBay, Home Depot, and Anthem Health Insurance were only a few of the many publicly disclosed breaches. The data breach of Anthem alone exposed the social security numbers of 80 million Americans.

The time has come for every manager and every employee in both government and private organizations to make cybersecurity a top priority in their daily work, and for leaders to be held accountable for negligent failures to protect information.

The American public and shareholders are demanding it. When criminal hackers gained access to some 40 million Target customer credit cards, the CEO and CIO were fired.

Although the OPM Director resigned in the wake of the OPM breaches, I am still not satisfied that the responsible parties have been held accountable for the failure of the agency to address known security vulnerabilities.

The most recent IG audit found that OPM still has 23 systems that have not been subject to a thorough security controls assessment. OPM does not even have a complete inventory of servers, databases and network devices in their system.

Just this week I met with newly appointed Senior Cyber and Information Technology Advisor Clifton Triplett and the OMB Senior Advisor on Cyber and National Security. I

look forward to working with my colleagues and all federal agencies to ensure we are protecting the identities of our employees, applicants, and their families.
The cyber criminals, "hacktivists", and state- sponsored cyber terrorists are getting more creative and bolder in their attacks.

The private sector has been at the forefront of dealing with these threats for some time, as both the target of many of these attacks and as the leaders in developing the technology and workforce necessary to counter cyber threats.

Visa, a global payment company, is preparing to open a new Cyber Fusion Center in my district just next week. This state of the art cyber facility brings together nearly 100 highly trained security professionals into one high-tech campus, and provides for collaboration both internally and with payments ecosystem partners -enabling information sharing, rapid response, coordinated command and control for defensive operations, and launching a real-time visualization of security events & response.

I look forward to hearing from our witnesses today, who are all innovative thinkers from the private sector. I hope we can take the lessons we learn from you today, and help apply them towards protecting our federal information systems and the sensitive and valuable information they contain.

Leaders in government and the private sector must work together to create a culture that ensures everyone considers cybersecurity a shared responsibility.

###

Chairwoman COMSTOCK. I now recognize the Ranking Member of the Research and Technology Subcommittee, the gentleman from Illinois, Mr. Lipinski, for his opening statement.

Mr. LIPINSKI. Thank you, Chairwoman Comstock and Chairman Loudermilk, for holding this hearing. I want to thank all the witnesses for being here today, and I look forward to hearing your testimony.

Chairwoman Comstock had mentioned in her opening statement the real need to make sure we do more in this area. We need to make sure that both in the public and private sector that people are held responsible for the hacks that do occur. We need to make sure that we have in place what we can do here, that Congress does what it can do to make sure that there is an incentive both in the public and private sector to try to avoid these hacks, this loss of information, so I'm very interested to hear more from our witnesses on this.

I am certainly pleased that we're holding our first hearing on cybersecurity, which is certainly an increasingly urgent challenge for our national security and the personal security of every American. It's important that we continue to hear from experts in government and the private sector about the latest developments with respect to both the risks that confront security in cyberspace, and the technologies and policies to combat those threats.

Our Committee plays an important role in both the technology side and the policy side, and this is an area in which Members have successfully collaborated across the aisle. In December 2014, Congress enacted the Cybersecurity Enhancement Act, a bipartisan research, education, and standards bill that I worked on with Mr. McCaul over several years. Over the last month, Congress enacted a cybersecurity law to promote information sharing and strengthen coordination between the private and public sectors. As a Committee and as Congress, we need to continue to confront these serious cyber threats.

Unfortunately, we continue to see an increase in major cyber-attacks in both the public and private sectors. In a hearing we held here in July, we heard about the significant breach at the Office of Personnel Management, in which the personal information of millions of current and former federal employees and job applicants was compromised, including some of us here. Highly sensitive security-clearance files were also compromised, making it not just a problem for all those individuals but a national security issue as well.

We have laws in place to address the security of federal information systems. The Federal Information Security Management Act, or FISMA, and subsequent amendments establish the necessary policies and procedures for the development of standards and protocols. NIST has an important role in this. But it is clear that federal agencies need to do a better job implementing NIST's standards and protocols, and that Congress needs to give them adequate resources to do so.

The private sector is also under constant threat from cyberattacks. In the case of large-size companies, a recent study conducted by the Ponemon Institute found that there was a 19 percent increase in cybercrimes between 2014 and 2015. The study also found that cybercrimes cause significant economic damage. For 2015, cyber attacks resulted in a total average cost of $15 million. While the threats continue to grow, many in the private sector are increasingly taking steps to protect their information systems and the personal information of Americans that they gather in their routine business.

To reduce our risk and improve the security of cyberspace, it will take the combined effort of the Federal government, the private sector, our researchers and engineers, and the general public. Although cyber attacks are becoming more sophisticated, often cyber attacks are successful because of human error, such as unknowingly opening a malicious email or allowing one's credentials to be compromised. Part of our effort must be to educate the public. Another part must be to better understand human behavior in order to make new tools and technologies more effective, such as the work being done at NIST and elsewhere to move beyond passwords.

I look forward to hearing from our witnesses today about industry cybersecurity best practices as well as opportunities for public-private partnerships that could help address our shared cybersecurity challenges. I'm also interested in hearing to what extent private businesses and organizations voluntarily implement FISMA standards developed by NIST, and how you may be participating in or benefiting from other efforts at NIST, including the Cybersecurity Center for Excellence and the Framework for Critical Infrastructure.

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

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT
Ranking Member Daniel Lipinski (D-IL)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
Subcommittee on Oversight
"Cyber Security: What the Federal Government Can Learn from the Private Sector"
January 8, 2016

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on cybersecurity. I want to thank all the witnesses for being here today and I look forward to hearing your testimony.

I am pleased that our first hearing of the year is on cybersecurity, an increasingly urgent challenge for our national security and the personal security of every American. It is important that we continue to hear from experts in government and the private sector about the latest developments with respect to both the risks that confront security in cyberspace, and the technologies and policies to combat those threats. Our Committee plays an important role in both the technology side and the policy side, and this is an area in which Members have successfully collaborated across the aisle. In December 2014, Congress enacted the *Cybersecurity Enhancement Act*, a bipartisan research, education, and standards bill that I worked on with Mr. McCaul over several years. And last month Congress enacted a cybersecurity law to promote information sharing and strengthen coordination between the private and public sectors. As a Committee and a Congress we need to continue to confront these serious cyber threats.

Unfortunately, we continue to see an increase in major cyber-attacks in both the public and private sectors. In a hearing we held here in July, we heard about the significant breach at the Office of Personnel Management (OPM), in which the personal information of millions of current and former federal employees and job applicants was compromised. Highly sensitive security-clearance files were compromised, making it not just a problem for all those individuals but a national security issue as well.

We have laws in place to address the security of federal information systems. The Federal Information Security Management Act, or FISMA, and subsequent amendments establish the necessary policies and procedures for the development of standards and protocols;

NIST has an important role in this. But it is clear that federal agencies need to do a better job implementing NIST's standards and protocols, and that Congress needs to give them adequate resources to do so.

The private sector is also under constant threat from cyberattacks. In the case of large-size companies, a recent study conducted by the Ponemon Institute found that there was a 19 percent increase in cybercrimes between 2014 and 2015. The study also found that cybercrimes cause significant economic damages. For 2015, cyber-attacks resulted in a total average cost of $15 million. While the threats continue to grow, many in the private sector are increasingly taking steps to protect their information systems and the personal information of Americans that they gather in their routine business practices.

To reduce our risk and improve the security of cyberspace, it will take the combined effort of the Federal government, the private sector, our researchers and engineers, and the general public. Although cyber-attacks are becoming more sophisticated, often cyber-attacks are successful because of human error, such as unknowingly opening a malicious email or allowing one's credentials to be compromised. Part of our effort must be to educate the public. Another part must be to better understand human behavior in order to make new tools and technologies more effective, such as the work being done at NIST and elsewhere to move beyond passwords.

I look forward to hearing from our witnesses today about industry cybersecurity best practices as well as opportunities for public-private partnerships that could help address our shared cybersecurity challenges. I'm also interested in hearing to what extent private businesses and organizations voluntarily implement FISMA standards developed by NIST, and how you may be participating in or benefiting from other efforts at NIST, including the Cybersecurity Center for Excellence and the Framework for Critical Infrastructure.

Thank you and I yield back the balance of my time.

Chairwoman COMSTOCK. Thank you, Mr. Lipinski.

I now recognize the Chair of the Oversight Subcommittee, the gentleman from Georgia, Mr. Loudermilk, for his opening statement.

Mr. LOUDERMILK. Well, thank you, Chairwoman Comstock, especially for continuing this important discussion on the security of our federal information systems.

I would also like to thank our witnesses for being here today to help us understand industry's best practices when it comes to cybersecurity. I look forward to hearing about lessons learned and how to apply those lessons to our federal systems to help prevent future cyber-attacks.

It is clear that our federal systems are not adequately protected. In fact, just this past summer, a witness from the Government Accountability Office before this Committee stated, "It is incumbent upon federal agencies to implement the appropriate security controls to mitigate those risks at a cost-effective and acceptable level, and we found out that agencies have not consistently implemented agency-wide information security programs to mitigate that risk effectively." When I asked that same witness to grade our federal cybersecurity, he gave it a D. A rating of D is not an acceptable grade.

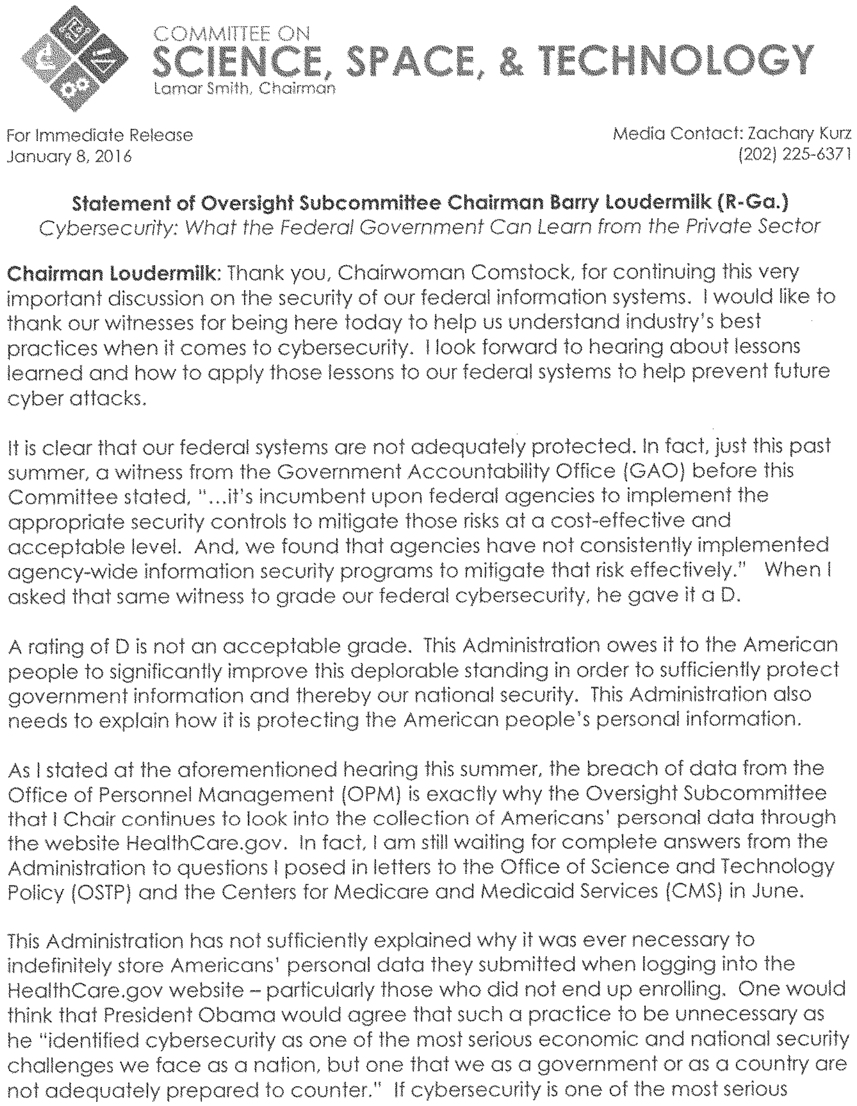
This Administration owes it to the American people to significantly improve this deplorable standing in order to sufficiently protect government information and thereby our national security. This Administration also needs to explain how it is protecting the American people's personal information. As I stated at the hearing this summer, the breach of data from the Office of Personnel Management is exactly why the Oversight Subcommittee that I chair continues to look into the collection of Americans' personal data through the website HealthCare.gov. In fact, I am still waiting for complete answers from the Administration to questions I posed in letters to the Office of Science and Technology Policy and the Centers for Medicare and Medicaid Services back in June. This Administration has not sufficiently explained why it was ever necessary to indefinitely store Americans' personnel—personal data they submitted when logging into the HealthCare.gov website, particularly those who did not end up enrolling. One would think that President Obama would agree that such a practice is unnecessary as he identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. If cybersecurity is one of the most serious challenges that this government faces, why on earth would the government ever consider storing all of this personal information indefinitely in data warehouses? As the Chairman of the Oversight Subcommittee, I will continue to ask questions and demand answers until we are satisfied that federal departments and agencies are making decisions in the best interest of protecting the personal information of all Americans. The safety and security of Americans and this Nation must be our number one priority.

Having continuously subpar security of our federal systems is embarrassing and must be rectified immediately. The delays must stop. It's time to finally do something about federal cybersecurity.

I look forward to the witnesses' testimony at today's hearing. I hope to learn more about the various industry best practices and lessons learned in hopes that it will shed light on what the government could and should be doing to protect our citizens from constantly evolving cyber threats.

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

[The prepared statement of Mr. Loudermilk follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Oversight Subcommittee Chairman Barry Loudermilk (R-Ga.)
Cybersecurity: What the Federal Government Can Learn from the Private Sector

Chairman Loudermilk: Thank you, Chairwoman Comstock, for continuing this very important discussion on the security of our federal information systems. I would like to thank our witnesses for being here today to help us understand industry's best practices when it comes to cybersecurity. I look forward to hearing about lessons learned and how to apply those lessons to our federal systems to help prevent future cyber attacks.

It is clear that our federal systems are not adequately protected. In fact, just this past summer, a witness from the Government Accountability Office (GAO) before this Committee stated, "...it's incumbent upon federal agencies to implement the appropriate security controls to mitigate those risks at a cost-effective and acceptable level. And, we found that agencies have not consistently implemented agency-wide information security programs to mitigate that risk effectively." When I asked that same witness to grade our federal cybersecurity, he gave it a D.

A rating of D is not an acceptable grade. This Administration owes it to the American people to significantly improve this deplorable standing in order to sufficiently protect government information and thereby our national security. This Administration also needs to explain how it is protecting the American people's personal information.

As I stated at the aforementioned hearing this summer, the breach of data from the Office of Personnel Management (OPM) is exactly why the Oversight Subcommittee that I Chair continues to look into the collection of Americans' personal data through the website HealthCare.gov. In fact, I am still waiting for complete answers from the Administration to questions I posed in letters to the Office of Science and Technology Policy (OSTP) and the Centers for Medicare and Medicaid Services (CMS) in June.

This Administration has not sufficiently explained why it was ever necessary to indefinitely store Americans' personal data they submitted when logging into the HealthCare.gov website – particularly those who did not end up enrolling. One would think that President Obama would agree that such a practice to be unnecessary as he "identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter." If cybersecurity is one of the most serious challenges that this government faces, why on earth would the government ever consider storing all of this personal information – indefinitely - in a data warehouse?

As the Chairman of the Oversight Subcommittee, I will continue to ask questions and demand answers until we are satisfied that federal departments and agencies are making decisions in the best interest of protecting the personal information of all Americans. The safety and security of Americans and this nation must be our number one priority. Having continuous, subpar security of our federal systems is embarrassing and must be rectified immediately. The delays must stop. It is time to finally do something about federal cybersecurity.

I look forward to the witnesses' testimony at today's hearing. I hope to learn more about the various industry best practices and lessons learned in hopes that it will shed a light on what the government could and should be doing to protect our citizens from constantly evolving cyber threats.

###

Chairwoman COMSTOCK. Thank you, Chairman Loudermilk.

And I now recognize the Ranking Member of the Subcommittee on Oversight for his opening statement.

Mr. BEYER. Thank you, Chairwoman Comstock and Chairman Loudermilk, for holding today's hearing. Thank you, witnesses, for spending Friday morning with us.

As we keep relearning after each new attack, cybersecurity is obviously a critical and daunting challenge. Today the data we create, store, access, and often share online contains information about almost every aspect of our lives. Our collective digital universe is composed of banking records, birth records, personal health files, government records, tax filings, on and on.

Last week, I was going on realage.com to see how long I was going to live, and now the cybersecurity attackers are going to know my cholesterol, my weight, the name of my dog, and the last year I had a cigarette. I took an Alzheimer's test last night online, which results I hope don't show up in my next campaign.

We electronically communicate with our kids' teachers about their academic achievements. I find that none of my kids will return my phone calls but they will text me right back. News flash: None of this information is secure, and immediate access to these digital connections provides tremendous advantages for businesses and consumers. In our family business, we're highly dependent on all the information we've gathered on our customers, the next time Congresswoman Bonamici needs an oil change on her Subaru, for example. It also offers abundant nefarious opportunities for cyber criminals, foreign governments intent on cyber espionage, and perhaps even more dangerous actors.

Protecting against known and emerging cyber threats is an ongoing enterprise that requires consistent vigilance and continuing adoption. Last year's OPM attack was a huge concern for all the federal workers that live in our districts across the country, and there were management and procedural failures at OPM that are now being addressed.

But nobody is immune to cyber attacks, not in the government and not in the private sector. According to Privacy Rights Clearinghouse, a nonprofit, nonpartisan, organization that tracks cyberattacks, in 2015 there were 17 reported breaches against .gov or .mil addresses that resulted in access to 27.8 million records. The big one there obviously was OPM. During the same time period, the private sector experienced 184 confirmed breaches that resulted in exposure of 131.5 million records. It's a huge problem for both sides.

I believe that sharing best practices to reduce IT vulnerabilities, educate federal workers is very important. I really look forward to today's hearing. I'm sure there are many lessons that we will learn from you today. I also look forward to the equal certainty that there is much that the private sector can learn from the government, especially the Department of Defense and our intelligence community.

So I look forward to today's discussion, and thank you so much for being with us.

Mr. Chair—Madam Chair, I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT

Ranking Member Don Beyer

House Committee on Science, Space, and Technology
Subcommittee on Environment
Subcommittee on Oversight
"Cyber Security: What the Federal Government Can Learn from the Private Sector"
January 8, 2016

Thank you Chairwoman Comstock and Chairman Loudermilk for holding today's hearing.

As we all know, and unfortunately keep relearning after each new attack, cybersecurity is a critical and daunting challenge. Today the data we create, store, access, and often share online contains information about almost every aspect of our lives. Our collective digital universe is composed of banking records, birth records, personal health files, government records, including tax filings and for some government workers, sensitive security background information. Communication that once happened in person or by phone is now online. We electronically communicate with our children's teachers about their academic achievements and social needs, and interact on a multitude of different digital social media platforms with our friends, family and colleagues. This should not come as a shock or news flash to anyone, but none of this information is fully secure.

Immediate access to these digital connections provides tremendous advantages for businesses and consumers, government agencies, educators and students, scientists, researchers, physicians and security analysts. But it also offers abundant nefarious opportunities for cyber criminals, foreign governments intent on cyber espionage, and other perhaps even more dangerous actors. Protecting against known and emerging cyber threats is an ongoing enterprise that requires consistent vigilance and continuing adoption of new operational methods and innovative technologies to thwart these escalating criminal activities and dangerous hazards in cyberspace.

Last year's announcement that the Office of Personnel Management - or OPM - suffered a major cyberattack was deeply concerning for having exposed the records of millions of records of federal workers. There were management and procedural failures at OPM that are now being addressed. But nobody is immune from cyber-attacks, not in the government and not in the private sector.

According to Privacy Rights Clearinghouse, a nonprofit, nonpartisan, organization that tracks cyberattacks, in 2015 there were 17 reported breaches against .gov or .mil addresses that resulted in access to 27.8 million records. During the same time period, the private sector, including commercial businesses, healthcare providers, and universities experienced 184 confirmed breaches that resulted in exposure of 131.5 million records.

I believe that sharing best practices to reduce IT vulnerabilities and educate federal workers, corporate employees, and consumers about the risks and threats of various cyber attacks' is an important endeavor. The point of today's hearing is to discuss what the government may be able to learn from the private sector. I am sure there are many lessons the private sector can offer the federal government and I look forward to hearing such recommendations from today's expert panel. However, I am equally certain that the federal government and its hard working IT workers and cybersecurity experts have expertise they can provide to the private sector to help improve their own security. The way I see it, this needs to be a partnership.

I look forward to discussing the importance of applying cybersecurity best practices and implementing innovative technologies at both our federal agencies and in the private sector with our witnesses today. I hope this is the first of many discussions on how we can work together to address critical cyber security issues as they expand and evolve in the future.

With that I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize the distinguished Chairman of the full Committee, Mr. Smith.

Chairman SMITH. Thank you, Madam Chair.

Last year, more than 178 million records of Americans were exposed in cyber-attacks. The breach of the Office of Personnel Management alone compromised the personal information of more than 20 million people, which included Members and staff of this Committee.

The United States is a top target for foreign countries. Cyber criminals and hacktivists exploit vulnerabilities in our networks and cyber systems to obtain valuable information. The number of cybersecurity incidents reported by federal agencies has increased over 1,000 percent in the last eight years. In 2014, more than 67,000 cyber-attacks were reported, and many others, of course, were not.

A number of federal agencies guard America's cybersecurity interests. Several are under the jurisdiction of the Science Committee. These include the National Science Foundation, the National Institute of Standards and Technology, the Department of Homeland Security's Science and Technology Directorate, and the Department of Energy. All of these agencies support critical research and development to promote cybersecurity and set federal standards.

However, it is clear that too many federal agencies, like OPM, fail to meet the basic standards of information security. More must be done to ensure agencies make cybersecurity a top priority.

Last year, audits revealed that 19 of 24 major federal agencies failed to meet the basic cybersecurity standards mandated by law yet the Administration has allowed deficient systems to stay online.

What are the consequences when a federal agency fails to meet its basic duties to protect sensitive information? What does it say to federal employees, not to mention our adversaries, when cabinet secretaries don't take cybersecurity seriously and fail to follow the most basic email security practices involving our country's classified information?

In the private sector, those who neglect their duty to keep the information of their customers secure are usually fired. In the federal government, it seems the only people penalized are the millions of innocent Americans who have their personal information exposed.

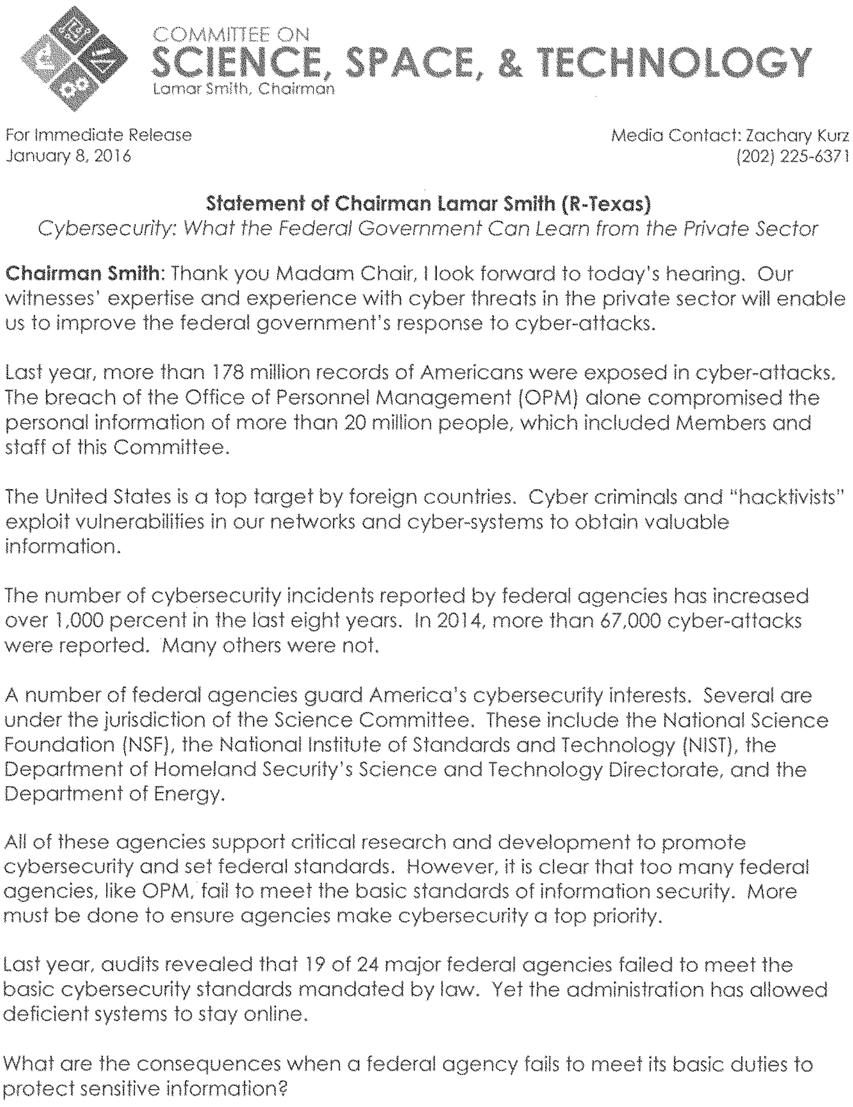
During the last Congress, the Science Committee approved the Cybersecurity Enhancement Act, which was signed into law. This law improves America's cybersecurity abilities and strengthens strategic planning for federal cybersecurity research and development. It supports NSF scholarships to improve the quality of our cybersecurity workforce. It also improves cybersecurity research, development, and public outreach organized by NIST.

Last month, a similar bill, the Cybersecurity Act of 2015, was signed into law. Very importantly, this bill encourages private companies to voluntarily share information about eminent cyber threats with each other as well as with the federal government.

The Science Committee will continue its efforts to support research and development to strengthen America's cyber defenses. I look forward to hearing from our witnesses today about what more we can do to support innovation and help set national standards and guidelines that will enhance our country's cybersecurity.

Thank you again, Madam Chair, and I yield back.

[The prepared statement of Chairman Smith follows:]



COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
January 8, 2016

Media Contact: Zachary Kurz
(202) 225-6371

Statement of Chairman Lamar Smith (R-Texas)

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Chairman Smith: Thank you Madam Chair, I look forward to today's hearing. Our witnesses' expertise and experience with cyber threats in the private sector will enable us to improve the federal government's response to cyber-attacks.

Last year, more than 178 million records of Americans were exposed in cyber-attacks. The breach of the Office of Personnel Management (OPM) alone compromised the personal information of more than 20 million people, which included Members and staff of this Committee.

The United States is a top target by foreign countries. Cyber criminals and "hacktivists" exploit vulnerabilities in our networks and cyber-systems to obtain valuable information.

The number of cybersecurity incidents reported by federal agencies has increased over 1,000 percent in the last eight years. In 2014, more than 67,000 cyber-attacks were reported. Many others were not.

A number of federal agencies guard America's cybersecurity interests. Several are under the jurisdiction of the Science Committee. These include the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Homeland Security's Science and Technology Directorate, and the Department of Energy.

All of these agencies support critical research and development to promote cybersecurity and set federal standards. However, it is clear that too many federal agencies, like OPM, fail to meet the basic standards of information security. More must be done to ensure agencies make cybersecurity a top priority.

Last year, audits revealed that 19 of 24 major federal agencies failed to meet the basic cybersecurity standards mandated by law. Yet the administration has allowed deficient systems to stay online.

What are the consequences when a federal agency fails to meet its basic duties to protect sensitive information?

What does it say to federal employees, not to mention our adversaries, when cabinet secretaries don't take cybersecurity seriously and fail to follow the most basic e-mail security practices involving our country's classified information?

In the private sector, those who neglect their duty to keep the information of their customers secure are usually fired. In the federal government, it seems the only people penalized are the millions of innocent Americans who have their personal information exposed.

During the last Congress, the Science Committee approved the *Cybersecurity Enhancement Act*, which was signed into law. This law improves America's cybersecurity abilities and strengthens strategic planning for federal cybersecurity research and development. It supports NSF scholarships to improve the quality of our cybersecurity workforce. It also improves cybersecurity research, development and public outreach organized by NIST.

Last month, a similar bill, the *Cybersecurity Act of 2015*, was signed into law. Very importantly, this bill encourages private companies to voluntarily share information about eminent cyber threats with each other as well as with the federal government.

The Science Committee will continue its efforts to support research and development to strengthen America's cyber defenses.

I look forward to hearing from our witnesses today about what more we can do to support innovation and help set national standards and guidelines that will enhance our country's cybersecurity.

###

Chairwoman COMSTOCK. Thank you, Mr. Chairman.

At this time I would now like to introduce our witnesses.

John Wood is Chief Executive Officer and Chairman of the Board for Telos Corporation, a leading technology company that addressees cybersecurity, secure mobility, and identity management for corporations and governments worldwide. Mr. Wood serves on the Boards of the Northern Virginia Technology Council, the Wolf Trap Foundation for the Performing Arts, home of the nationally acclaimed Wolf Trap Institute for Early Learning through the Arts and its Early STEM Arts Program. He is also the founding chairman of the Loudoun County CEO Cabinet and served for five years as Chairman of Loudoun County's Economic Development Commission. Prior to joining Telos in 1992, Mr. Wood worked on Wall Street after earning his degree in finance and computer science at Georgetown University. I know he also is very active in STEM education throughout Loudoun County in our district in getting young people engaged and involving them personally, I know both with your company and with our school system. We appreciate all you do in that area.

Dr. Martin Casado is a VMWare Fellow and Senior Vice President and General Manager for the Networking and Security Business Unit. Dr. Casado joined VMWare in 2012 when the company acquired Nicira, of which he was Co-Founder and Chief Technology Officer. Dr. Casado has previously held a research position at Lawrence Livermore National Laboratory, where he worked on network security in the information operations assurance center. Dr. Casado has been recognized as one of the industry's leading innovators and has been featured as one of Business Insider's 50 Most Powerful People in Enterprise Tech, Forbes Next Generation Innovators, and Dr. Casado received his master's and Ph.D. from Stanford.

Mr. Ken Schneider serves as Vice President of Technology Strategy at Symantec, where his focus is on driving an overall technology strategy across the company. He was previously Chief Technology Officer of the Enterprise Security and Security and Data Management Groups. Prior to joining Symantec, Mr. Schneider served as CTO and VP of operations for Brightmail, the leading anti-spasm software company that was acquired by Symantec. Before Brightmail, Mr. Schneider South Beach Software, a software consulting company that developed products for the professional video market. He also received a master of science in mechanical engineering from University of California Berkeley and a bachelor of science in engineering from Swarthmore.

Mr. Clinton is the President and Chief Executive Officer of the Internet Security Alliance, a multisector trade association focused on cyber thought leadership, policy advocacy, and promoting sound security practices for corporations. Mr. Clinton has widely published on cybersecurity and is the principal author of the Cyber Risk Handbook for corporate boards published by the National Association of Corporate Directors in 2014 and endorsed by the Department of Homeland Security in 2015. The NACD also named Mr. Clinton as one of the 100 most influential individuals in the field of corporate governance last year. Mr. Clinton is in demand internationally, having spoken in Europe, Asia, and Latin America, and we are glad to have him here today.

In order to allow time for your discussion, please limit your testimony to five minutes, and then your entire written statements, which I know are more extensive and have lots of good information that we'll have in our public record, and since we're on C–SPAN today, I would encourage the public to also look at those full statements to get more information there, and with that, I will recognize Mr. Wood for five minutes to present his testimony.

TESTIMONY OF MR. JOHN B. WOOD, CHIEF EXECUTIVE OFFICER AND CHAIRMAN, TELOS CORPORATION

Mr. WOOD. Thank you. I'd like to thank Chairwoman Comstock and the other Chairs and Ranking Members for the invitation to share some thoughts on behalf of Telos Corporation on industry best practices for cybersecurity and risk management.

As I noted in my written testimony, Telos protects the world's most security-conscious enterprises, providing our customers with solutions and services for cybersecurity, secure mobility, and identity management.

The first point I'd like to highlight is that all enterprises, public and private, need to emphasis cyber hygiene in their day-to-day operational practices and employee training.

Why do I make this first point? Because the 2015 Verizon data breach investigations report found that the overwhelming common denominator in security incidents is people. Nearly all of the security incidents Verizon cataloged might have been avoided if organizations had taken basic steps to help their employees follow simple cybersecurity precautions.

Here are five basic steps that organizations should take to help better protect themselves from attacks. First, establish and enforce cybersecurity policies and procedures. Second, include effective password management practices. Third, require regular security awareness training. Fourth, implement timely updates and patches to manage vulnerabilities. And fifth, to use up-to-date endpoint security solutions. These five basic steps serve as the foundation for a strong cybersecurity program. Every IT security professional knows them, and yet the importance of following through with them cannot be overstated.

Further, these practices must be embraced in the boardroom, and by management, so that a culture of cybersecurity is created throughout the organization from the top town.

That being said, every organization with high-value digital assets needs to assume it has already been breached or will be. This leads to my second point, and that is that incident response and remediation are just as important to organizations as cyber defense and depth strategies.

Telos has developed a rigorous framework for incident response with essential steps like preparation, containment, eradication and recovery, which we use ourselves and implement for our customers.

Further, it isn't realistic to expect every organization to have the time or financial and human resources needed to successfully defend everything. That's why management is so critical to effective cybersecurity. Risk management involves identifying, evaluating, and either accepting or mitigating uncertainty in decision making.

Private and public sector organizations need to make cost-benefit choices about which systems to defend and how to defend them based on the likelihood of an asset being attacked, the value of the asset being attacked, the cost of defending the asset, and the cost of losing the asset. That approach is reflected in the continuous diagnostic and mitigation program established by Congress "to provide adequate risk-based and cost-effective cybersecurity and more efficiently allocate cybersecurity resources." This continuous diagnostic to mediation program, or CDM program, extends continuous monitoring into the areas of diagnostics and mitigation while acknowledging that risk management is called for when you have to meet nearly infinite needs with finite resources.

That's also the value of initiatives like the NIST risk management framework and the NIST cybersecurity framework. They put cybersecurity solutions and best practices in the context of risk management and compliance, which brings me to my third point. The standards in the NIST cybersecurity framework are very good but they cannot succeed unless companies follow them. We should be looking for ways that market forces can incentivize companies to voluntarily take the strongest possible actions to protect themselves, which includes following the NIST standards and best practices.

The various critical infrastructure sectors are just that: critical. They're so important to our national defense, our economy, and our way of life that it's imperative government and private sectors encourage organizations in these sectors to use best security practices.

One promising area of incentivizing companies is tied to the growth of the cyber insurance market. The Commerce Department has described cyber insurance as "an effective market-driven way of increasing cybersecurity." The Treasury Department has also suggested that the increasing demand for cyber insurance may help drive private sector policyholders to adopt the NIST cybersecurity framework. As insurance companies get their arms around the cybersecurity actuarial data they accumulate with each new breach, they'll want to have insights into what their clients are doing to protect themselves. Are they applying sufficient ongoing protection for their systems and data? Are they using the NIST framework or an equivalent standard? In fact, insurance companies may well require their clients to adopt the NIST framework in order to demonstrate insurability and reduce their premiums. When that happens, we could see greater market-based pressure brought to bear that will effectively require companies to do the same. So market forces and the fear of legal liability may make NIST voluntary guidelines the de facto standards for companies to demonstrate to insurers or in court that they've exercised all due care to protect their customers and their assets.

One additional point: Cybersecurity is just too important to do on the cheap. Overreliance on "lowest price technically acceptable" contracts can be very risky in a field that has so little room for error.

Similarly, our fifth war-fighting domain, cyberspace, must be appropriately funded. U.S. Cyber Command has been funded at a level this year that represents a mere 1/1000ths of the overall DOD budget. By contrast, just four banks—JP Morgan Chase, Bank of America, Citibank and Wells Fargo—are spending three times the amount on cybersecurity. JP Morgan, after they got hacked, decided to double their IT security spend from $250 million a year to $500 million a year, more than all of Cyber Command. The financial sector is an example of the private sector taking its cybersecurity risk management responsibilities very seriously and devoting the resources necessary to protect themselves.

Again, I appreciate the opportunity to share with you Telos's perspective, and I'd be glad to answer any questions. Thank you.

[The prepared statement of Mr. Wood follows:]

STATEMENT

OF

JOHN B. WOOD

CHIEF EXECUTIVE OFFICER & CHAIRMAN

TELOS CORPORATION

HOUSE SCIENCE, SPACE & TECHNOLOGY SUBCOMMITTEES
ON
RESEARCH & TECHNOLOGY AND OVERSIGHT

HEARING ON

"CYBER SECURITY: WHAT THE FEDERAL GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR"

JANUARY 8, 2016

Chairman Smith, Ranking Member Johnson, Chairwoman Comstock, Ranking Member Lipinski, Chairman Loudermilk, Ranking Member Beyer, members of the Committee. My name is John Wood. I am CEO and Chairman of the Board of Telos Corporation, a cyber security company headquartered in Ashburn, Virginia.

Telos Corporation empowers and protects the world's most security-conscious enterprises with solutions and services for continuous security assurance of individuals, systems, and information. Our offerings include cyber security solutions and services for IT risk management and information security; secure mobility to protect globally connected enterprises; and identity management to establish trust in personnel and continuously monitor for insider threats. We serve customers in the military, intelligence and civilian agencies of the federal government, allied nations, and commercial organizations around the world.

I have been with Telos for 23 years, including serving the past 20 years as CEO. Twenty years is a long time in any business but in the rapidly changing world of cyber security, it often seems more like a hundred years.

I appreciate the invitation to discuss industry best practices from Telos' perspective, and to share with you my observations regarding how those private sector practices can and should be applied to the public sector. As a cyber security company and as a contractor that does a significant amount of work with military, intelligence and civilian agency customers, this is obviously a topic of great importance to Telos.

Last summer's disclosure of the massive OPM breach, on which you and other committees held hearings, highlighted for me an important lesson for executives in both the public and private sectors. That is, in every organization, whether it is a commercial entity or a government agency, the command chain needs to be intimately aware of cyber security issues; this means risk management needs to be overseen at the highest level. It has to be that way and it is irresponsible if such oversight is not happening. Senior management must receive frequent reviews and reports of the organization's cyber vulnerabilities, along with plans for remediation. Issues of cyber risk management and information security can no longer be solely shouldered by an organization's chief information security officer (CISO). Top executives must have a basic knowledge of their organization's cyber risk and take responsibility for the solution.

This also highlights the stated purpose of this hearing: what can the public sector learn from the private sector? In addition to having strong leadership at the top on cyber security issues, there has to be a commitment to a culture of cyber hygiene at the top that permeates through the entire organization. That's what we do, that's what many of our peers do, and that's what government agencies must do as well.

It is the responsibility of management to ensure that basic cyber security training is provided throughout an organization. This is borne out by the **2015 Verizon Data Breach Investigations Report** (DBIR), which said that "the common denominator across the top four patterns [of security incidents] — accounting for nearly 90% of all incidents — is people." Let's be clear what this means — the Verizon study found that a majority of security incidents reported may have been avoided if employees had taken *basic* cyber security precautions, like implementing stronger passwords and two-factor authentication, patching software, and knowing how to recognize the signs of a phishing attack. Having a more educated employee base doesn't mean an entity is impervious to being hacked, but it does *significantly* decrease the chances and frees up resources for defending against the more sophisticated attacks.

The basics of information security cannot be ignored in day-to-day operations. A few years ago, one of our security experts came up with five basic steps that organizations should be taking to better protect themselves from attacks. These **risk management practices** are things we do, and we believe all organizations – public and private – should be doing them as well.

The first has to do with the basic **passwords** people use, regardless of whether two-factor authentication is used. Is eight characters still a good idea? What about nine, 10, or 20 characters? We need to strike the right balance between usability and security. The problem is, if a user gets a 20-character password, odds are they will write it down at their work station, or worse yet, put it in a file called 'passwords.txt' in their home directory. So there needs to be a balance – users need to have passwords that are as long as they can possibly remember without having to write it down somewhere or leave it in a computer file that can be a gold mine for hackers.

There are several ways to create strong passwords. One way is to use pass-phrases, which are easier for users to remember. Another approach is to use the first letter of every word in a phrase or sentence (use upper and lower case letters and numbers and special characters to replace letters when possible). You need strong passwords for all your employees, and they need to be diligent about making sure the bad guys can't guess their passwords.

The second step is **security awareness training**. It may not always succeed, but security training can help reduce the probability and number of data breaches that are attributable to human error, as noted in the Verizon report. Employees must be trained to know that if something is wrong they should report it – even if something only *appears* to be wrong, they should report it. A security awareness program operates just like an anti-terrorism operation; it cannot fully function without help and reports from the public. If you see something, say something. An unaware employee population will fall for phishing attacks, and will never report it or know they are compromised. That's why we regularly perform penetration test exercises on our own employees – not just to catch anyone who is deficient in their security practices but to embed in every employee the need to be vigilant and exercise caution, even when an incoming email seems plausible. In sum, awareness training may not provide complete protection, but it is part of the equation that must be addressed by every organization.

Patch/vulnerability management is the third, and some say the most important, step that organizations must take. But like most security functions, patch management is only as good as the people behind it. Patches of critical vulnerabilities should be required within a short window.

The fourth step involves making sure an organization has a working enterprise-level **malware detection/prevention solution** that keeps machines and devices up to date with the most current definitions or software. According to Symantec, there are nearly one million new malware variants introduced every three days! That's why, like patch management, anti-malware updates are critical. Similarly, IT departments need to review the security logs daily to check for anomalies and promptly report problems to top management.

Finally there have to be cyber security **policies and procedures** in place that are strongly supported, reviewed and enforced. Too often organizations view policies and procedures as a checkbox paper drill, which is a huge mistake. Good policies and procedures eliminate confusion in the aftermath or during an otherwise chaotic event.

As part of this, private and public sector organizations need strong, qualified individuals in the right positions. Unfortunately, many companies and organizations are settling for individuals who can talk their way into a Chief Information Security Officer (CISO) or Security Director role without having any real experience, or are asking others to look at the job as an "other duties as assigned" role. Having credentials, a strong background and practical experience is critical. Whether we are talking about a commercial company or a government agency, it is critical to have the right person in a position to inform executive leadership about real risks and the appropriate steps to mitigate them.

These five elements – strong passwords, security awareness training, patch and vulnerability management, malware prevention and detection solutions, and policies and procedures – serve as the foundation for a strong cyber security risk management program. We believe in them, and we follow them. This is not something extra we *ask* of our employees – it's something we absolutely require.

Looking past these five basic steps, one additional item that should not be overlooked is encryption. Without encryption, laptops, mobile devices and USB sticks that are lost can easily lead to a data breach. Encryption of sensitive information is equally important whether dealing with web applications, communications or a database. A note of caution with respect to encryption; it is not a silver bullet. If valid credentials are entered into the web application it must decrypt the data for the end user to be able to manipulate or consume the data. This is why it is critical that administrative access is limited and that web application vulnerabilities are continuously looked for, identified and remediated.

It's important to recognize that no one process or security software is fool-proof. That's why we also advocate a defense-in-depth approach, which means protecting a network with multiple security mechanisms. If one mechanism fails, another is in place to thwart the attack. It's similar to fortifying a government or even a sensitive private sector installation. You build a secure facility and have armed guards on the perimeter, but if a truck rams the gate you need to have additional protections on the inside of the complex as well. It's a layered security model. The more layers in place, the harder it is for an attacker to infiltrate. Having a web application firewall sitting behind a network-based firewall makes an attacker work twice as hard. Having the system hardened with anti-malware creates yet another opportunity for the security defenses to prevent an impending attack.

Once a strong risk management program is in place, there is an equally critical task facing organizations: *How and when to respond to and recover from an incident.* Our folks came up with some common steps of **incident response** that serve as a helpful guide for us, and should be used by government agencies as well. These are:

1. **Preparation** – Prepare for an incident by opening lines of communication, having the proper documentation, and implementing an incident response team.
2. **Identification** – Next, answer the following question: Has something deviated from the norm causing an incident?
3. **Containment** – Prevent further damage and assess the scope of the incident.
4. **Eradication** – Remove and restore affected systems. Monitor fixes to assure malicious software and bad actors are removed.
5. **Recovery** – Bring systems safely back into production.
6. **Lessons Learned** – Identify who, what, where, why, and how the incident happened. What needs to be improved? What security policies and procedures need to be updated?

Underlying this strategy is continuous diagnostics and mitigation (CDM). We used to only talk about "continuous monitoring," which Telos has been involved with for many years and which, as the committee stated in its announcement for this hearing, was cited recently by OPM's Office of the Inspector General as being a basic security process where OPM's efforts have fallen short. But as noted above, the mitigation steps which an enterprise takes are also critical.

Continuous monitoring solved one problem (detection) but left out another (remediation). As organizations embraced the concept of continuous monitoring, continuous response remediation was the obvious next step. Extending the continuous monitoring framework to include automated methods for triggering remediation and response activity is essential. So now the more accurate and complete operative phrase is CDM. That is the current priority of Congress and of the Department of Homeland Security, which notes on its **website** that, "Congress established the CDM program to provide adequate, risk-based, and cost-effective cyber security and more efficiently allocate cyber security resources."

This hearing was also originally called to address **whether the voluntary cyber security standards (the "Framework") put forth by the National Institute of Standards and Technology (NIST) can truly be effective.** We continue to believe that the various critical infrastructure sectors are so important to our national defense, our national economy and our way of life that the government needs to do everything it can to promote best cyber security practices, such as those put forth by NIST. Most businesses would prefer that the government impose the fewest possible requirements on them. But how many breaches will it take before it is recognized that allowing the private sector – and especially critical infrastructure companies – to choose the path of least resistance creates an opportunity that might put our citizens' personal information at risk, put our critical infrastructures at risk and put our national economy at risk?

The hard reality is that the current NIST standards are purely voluntary, in part due to recognition by the Administration that there is insufficient support in Congress and the private sector to mandate stronger action. Various proposals to require stronger action were blocked in Congress a few years ago, and nothing seems to have changed. By comparison, the German Parliament last year passed legislation requiring critical infrastructure institutions to implement minimum information security practices or face fines. Once additional implementing legislation is passed, more than 2,000 essential service providers will have two years to comply with the new requirements. The German agency charged with enforcing these requirements will also be given the resources to expand to cover these new obligations, which will include evaluating reports of possible cyber-attacks on critical infrastructure.

Since Congress and the Administration have not taken the same strong steps that Germany is now taking, everything possible must be done to incentivize companies to *voluntarily* take the strongest possible actions to protect themselves, which includes following the NIST standards. Make no mistake, the NIST standards are very good...but companies must follow them even though they are voluntary.

One promising area of incentivizing companies to take strong steps on their own is the growth of the cyber insurance market. One of our experts noted several years ago that, as we see more frequent cyber security breaches, the cyber insurance industry will mature with each new data point it collects, and thus be able to more easily determine appropriate coverage, premiums, etc. Moreover, as insurance companies get their arms around this cyber security actuarial data, they will also want to have insight to what their clients are doing to protect themselves from cyber attacks. That is, are their clients employing adequate controls and security practices? Are these organizations applying sufficient ongoing care in the protection of their systems and data? Are their clients utilizing the NIST cyber security framework standards which, while voluntary, are nonetheless standards insurance companies can encourage, incentivize or even require their customers to follow? If that happens, and if it happens more frequently, then we could see greater market pressure brought to bear to effectively "require" other companies to do the same.

That is certainly better than allowing companies to do the bare minimum to protect themselves and those who do business with them. We need them to do the most they possibly can, not the least. In this way, market forces and the fear of legal liability will make these voluntary standards the de facto standards for companies to demonstrate to insurers or in court that they have exercised all due care to protect their assets and customers.

This rescheduled hearing also now seeks **feedback on the recently enacted Cybersecurity Act of 2015**, which was included in the Consolidated Appropriations Act to fund federal departments and agencies for the remainder of Fiscal Year 2016. As the committee members know, this law provides certain incentives to encourage private sector companies to voluntarily share cyber threat information with the federal government and/or with other private sector companies. We believe this new law overall is a net positive – threat information sharing is a good goal...but in practice it is much more complicated and it is difficult to achieve effective results.

Our first concern about the new law is, like the NIST Framework discussed earlier, it doesn't go far enough because of its purely voluntary nature. As has been shown in the experiences of those who participate in Information Sharing and Analysis Centers (ISACs), some companies just don't want to participate and disclose information about any weaknesses or vulnerabilities they might have. It's human nature not to want to disclose bad news to stockholders, investors, customers, and others if they don't have to – some companies will want to privately address any problems, without the inherent "bad publicity" of disclosure. The same holds true with respect to limited disclosure of confidential threat information. The Securities and Exchange

Commission has been making an effort to require greater disclosure of breaches, but timely disclosure to the government or other companies of confidential vulnerability or threat information is another matter. If a company chooses not to participate, it may be withholding vital threat information and thus putting other companies and individual citizens at risk.

Ironically, the law actually may create a "Catch 22" – some organizations may share *too much* information in an attempt to maximize liability protections, potentially resulting in too much data being shared and potentially putting personally identifiable information (PII) at risk.

Only time will tell if this latter concern is borne out, but we continue to believe the former concern about the law's purely voluntary nature is a very real one – it only takes one company's failure to act voluntarily to put many others at risk. We believe that, as with the NIST Framework, stronger market force incentives will be needed to encourage greater participation.

While it is not within the scope of this hearing, one final area I would like to address in this written statement is the need for the United States government to adequately fund cyber and information security. Making cyber security a priority to make our nation secure means making sure the government buys the best cyber security solutions it can get, not the cheapest. The **Lowest Priced Technically Acceptable** (LPTA) contracting environment we find ourselves in today often leads to awarding critical contracts to lowest cost bidders. The government should be looking for the best *value*, especially when it comes to cyber security. Congress needs to ask each agency what they need to properly protect their systems and then fund it.

Neglecting to properly fund our nation's cyber defense is severely shortsighted. Several years ago, our Government leaders argued correctly that cyber was the fifth warfighting domain along with land, sea, air, and space. Arguably, cyber is the most difficult domain to defend, and yet, we continue to undercut it, undermining our national security.

As an example, the President's proposed Fiscal Year 2016 Budget allocated $560 billion for the Department of Defense. Of that $560 billion, the Army was to be given $146 billion, the Navy $152 billion, and Air Force about the same. By comparison, the U.S. Cyber Command, with its incredibly challenging responsibilities to protect the fifth warfighting domain, was allotted about $462 million – less than 1/1000 of the total DoD budget. This funding disparity did not significantly change in the final FY 2016 appropriations legislation enacted in December. This failure to provide the funding needed to meet the cyber challenge applies to both military and civilian departments and agencies. As a result, we are vulnerable throughout the government.

Many private companies understand the challenges of protecting themselves from cyber threats, and are taking action. Financial services firms in general are especially battening down their hatches; they see the cyber risk and are being responsive to their customers and stakeholders. ***Forbes* recently summarized various media accounts of such actions**, noting that J.P. Morgan Chase & Co. expects its cyber security spending to be around $500 million in 2016, more than double the $250 million it spent in 2014. *Forbes* also reported that Bank of America Corp. CEO Brian Moynihan said previously his company would spend $400 million on cyber security in 2015, that Citibank's IT security budget reportedly tops $300 million, and that Wells Fargo is reported to spend roughly $250 million a year on cyber security. These institutions understand that devoting the resources necessary to protect their systems is absolutely critical.

Such expenditures produce results. According to a **recent Veracode report** comparing the state of software security by industry vertical, **government agencies fix fewer than one-third of all detected [software security] problems ... by comparison, financial services fixed 81% of detected problems, while manufacturing fixed 65%.** In light of the variance in funding levels between the government and private industry, it is no surprise that once detected, two-thirds of the software security problems in government systems are left unresolved. Private industry is funding cyber security like they're taking the issue seriously. The federal government is not.

Defending our nation in cyberspace requires a long-term national effort and commitment, much like the Space Race -- we have the equivalent of a cyber-race to the moon on our hands, and we are falling behind. This is the reality, and our Government leaders and Congress need to stop just talking cyber, and to start appropriately funding it.

In closing, on behalf of Telos, I appreciate this opportunity to share with you our perspective on these important issues, and I'd be glad to answer any questions you might have.

# # #

John B. Wood
Chief Executive Officer and Chairman of the Board
Telos Corporation

John Wood is chief executive officer and chairman of the board for Telos Corporation, a leading technology company addressing the critical areas of cybersecurity, secure mobility, and identity management for corporations and governments worldwide. Prior to joining Telos in 1992, Wood worked on Wall Street after earning his degree in finance and computer science at Georgetown University.

In 2014, Mr. Wood was appointed by Gov. McAuliffe to serve on the Virginia Cyber Security Commission. Established by executive order, the commission is designed "to bring public and private sector experts together to make recommendations on how to make Virginia the national leader in cybersecurity."

Mr. Wood serves on the boards of Northern Virginia Technology Council (NVTC) and Wolf Trap Foundation for the Performing Arts, home of the nationally acclaimed Wolf Trap Institute for Early Learning through the Arts and its Early STEM/Arts program. Mr. Wood is also an active member of the business community, championing the concept of civic entrepreneurship. He is the founding chairman of the Loudoun County CEO Cabinet and served for five years as chairman of Loudoun County's Economic Development Commission.

In 2012 Mr. Wood was named Chairman of the Board of Directors for the Tragedy Assistance Program for Survivors (TAPS), the national organization providing compassionate care for the families of America's fallen military heroes. He served ten years on the board of directors of Project Rebirth, a nonprofit committed to supporting health and healing among victims of tragic loss. The organization's award-winning documentary film, *REBIRTH*, employs time-lapse photography of the rebuilding of the Freedom Tower and a "human time lapse" of the journeys of nine people whose lives were dramatically affected by the events of 9/11. A portion of the film is on permanent display at the National 9/11 Museum, and a digital archive of over eight hundred hours is available at the Library of Congress and used by numerous colleges and universities in programs to facilitate healing, foster hope, and build resilience.

Chairwoman COMSTOCK. Thank you.

And now we'll hear from Dr. Casado.

TESTIMONY OF DR. MARTIN CASADO, SENIOR VICE PRESIDENT AND GENERAL MANAGER, NETWORKING AND SECURITY BUSINESS UNIT, VMWARE

Dr. CASADO. Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and other Members of the Committee, thank you for the opportunity to testify today. I'm super thrilled to be here.

I'm Martin Casado, Senior Vice President and General Manager of Networking and Security at VMWare. VMWare is the fourth largest software company in the world with 2014 revenues of over $6 billion and over 18,000 employees.

The nature of security breach at the Office of Personnel Management was not particularly unique. Hackers were able to penetrate perimeter networks' security systems and gain access to OPM and Department of Interior systems where they were free to access and steal sensitive data over a period of several months. Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be doors to the network. These doors allow authorized users access to network systems and prevent unauthorized users from entering a network or data center.

However, perimeter security is a single point of entry that must be breached or circumvented in order to enter the data center network. Once the intruder has passed the perimeter, there's no simple means to stop malicious activity from moving throughout the data center. In many cases, the response from companies, agencies, and network security vendors is to add more security technology to the perimeter, which ignores the structural issue, creating basically a Maginot line.

VMWare submits three salient points for consideration. One: Every recent agency breach has had one thing in common: the attacker, once inside the perimeter security, was able to move freely around the agency's network. Two: Perimeter-centric cyber security policies, mandates, and techniques are necessary, but insufficient and ineffective in protecting U.S. government cyber assets alone. Three: These cyber-attacks will continue, but we can greatly increase our ability to mitigate them and limit the damage and severity of the attacks when they do.

So in today's legacy networks, there are a lot of perimeter-centric technologies that are designed to stop an attacker from getting inside a network. Clearly, this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone who does not have a key. However, once the door is forced open or breached, the unauthorized actor is free to move throughout unabated.

In order to effectively prevent an attacker from moving freely around the network, agencies must compartmentalize their existing network perimeter security by adding zero trust or micro-segmented network environments within the data center. A zero trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems or applications within the data center network. When a user or system breaks the rules, the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks, limiting the intruder's ability to move around freely within the house significantly. This mitigates the magnitude of a perimeter security breach, or break-in. These new approaches are already the gold standard in commercial industry and need to become the gold standard across the federal government.

VMWare has seen many government agencies conclude that the most effective means of mitigating the potential for a breach is to build a new network or data center called a "greenfield" environment with enhanced security protocols. Agencies reach this conclusion because existing data centers, or "brownfield" environments, are assumed to be compromised and unsalvageable. This is a legitimate strategy. However, it fails to address the persistent security threat to existing cyber infrastructure.

There are two main issues with this approach. Existing networks or data centers continue to operate while the new environment is being provisioned, which leaves sensitive data vulnerable to continuing attack. It can take months or years to stand up a new greenfield environment. As we've seen, this is what happened with the attack at OPM. They were building a new, enhanced network but the attack occurred on the existing system. Without clear cyber security guidelines mandating new software based security strategies that go beyond perimeter-centric security, the new environments are subject to attack as soon as they become operational.

In an era of constrained resources and imminent threat, this approach is insufficient and untimely. Agencies have the ability today to upgrade the security posture of their existing cyber infrastructure and add zero trust software defined solutions that are inherently more cost-effective than new, expensive hardware-based solutions. By deploying these technologies within our nation's existing networks and data centers, agencies can avoid billions of dollars of additional investment in new greenfield infrastructure when the compelling driver for a greenfield investment is strictly security related.

Thank you very much for the opportunity to testify today, and I look forward to answering the Committee's questions.

[The prepared statement of Dr. Casado follows:]

Testimony

Statement for the Record

Martin Casado, Senior Vice President

Networking and Security Business Unit

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Science, Space, and Technology

Cyber Security: What the Federal Government Can
Learn from the Private Sector

January 8, 2016

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and Members of the Committee, thank you for the opportunity to testify today. I am Martin Casado, Senior Vice President and General Manager of Networking and Security at VMware. I have a PhD in computer science from Stanford University and began my career at Lawrence Livermore National Laboratory where I worked on network security in the Information Operations Assurance Center (IOAC).

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over $6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Federal Government, the Civilian agencies, the Department of Defense, and the Intelligence Community as well as state and local governments. The company is headquartered in Silicon Valley, and given the Committee's leadership; I'd like to acknowledge we have a significant presence in Virginia and Georgia along with approximately 140 other offices throughout the world.

VMware is a leading provider of software-defined solutions that make data centers across the globe operate more efficiently and securely and allow both government and commercial organizations to respond to dynamic business needs. In 2012, it acquired the company I co-founded, Nicira, which greatly expanded VMware's capabilities in cyber security. Today, VMware is providing enhanced security to commercial and government customers globally through its pioneering role in redefining how we build and secure networks and data centers.

Cyber-Attacks: Clear and Persistent Threat to the U.S. Government

The U.S. Government is dependent on a vast cyber world of interconnected IT networks, data centers, the Cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated Census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber-systems has reaped immeasurable benefits for the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern day functions of Government, sophisticated and aggressive cyber-attacks perpetuated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. Well-publicized cyber-attacks have targeted the U.S. Postal Service, the U.S. Department of Commerce, the U.S. State Department, the Internal Revenue Service, and other agencies. In one of the largest cyber-attacks on a U.S. agency, and the reason for this important joint hearing, the Office of Personnel Management (OPM) suffered what appears to be one of the most damaging breaches of information ever on government workers. As you know, the OPM breach has potentially compromised the personal data and security of over 21 million current and former federal employees and has likely compromised our national security, national defense, and national intelligence posture(s). This breach has put our nation's blood and treasure at risk.

The recent attacks on our Government and within the private sector have had one thing in common: the attacker, once inside the network perimeter security, was able to move freely around the victim's network.

Given the recent string of cyber-attacks on our government, it is not a surprise that our collective trust in our cyber infrastructure, on which agencies are so dependent, is at risk. Without doubt, we are currently engaged in an escalating cyber arms race with entities that are methodical, sophisticated, and effective. They will continue to probe our cyber infrastructure for vulnerabilities and they will continue to exploit our agency's networks whenever possible.

It is clear to our nation and to those who perpetuate these attacks that the way in which we protect our national cyber infrastructure, the way in which we design and deploy cyber security systems across federal agencies, is insufficient.

As is apparent from publicized accounts, the nature of the security breach at OPM is not particularly unique. Hackers were able to penetrate perimeter network security systems and subsequently gain access to OPM and Department of Interior systems, where they were free to access and steal sensitive data over a period of several months. Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be "doors" to the network. These systems allow authorized users access to networked systems and prevent unauthorized users from entering a network or data center. However, perimeter security is a single point of entry (a single perimeter: firewall + additional security systems like intrusion prevention or advanced attack detection) that must be breached or circumvented in order to enter the data center network. Once the intruder has passed the perimeter security there is no simple means to stop malicious activity from propogating throughout the data center. In many cases, the response from agencies and network security vendors is to add more security technology to the perimeter, which ignores the structural issue.

Mitigating the economic, political, and social damage to our nation from these types of cyber-attacks demands that we change the way we build, operate, and secure our Government's mission critical IT infrastructure.

VMware submits three salient points for consideration:

1) Every recent agency breach has had one thing in common: the attacker, once inside the perimeter security, has been able to move freely around the agency's network.
2) Perimeter-centric cyber security policies, mandates, and techniques are necessary, but insufficient and ineffective in protecting U.S. Government cyber assets alone.
3) These cyber-attacks will continue, but we can greatly increase our ability to mitigate them and limit the damage and severity of the attacks when they do.

Address the Threat: Immobilize the Attacker Inside the Network

In today's legacy networks, in government as well as the commercial sector, there are a lot of perimeter-centric technologies that are designed to stop an attacker from getting inside a network – clearly this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone who does not have a key. However, once the door is forced open (hacked or breached), the unauthorized actor is free to move throughout (laterally) unabated.

In order to effectively prevent an Attacker from moving freely around the network, agencies must compartmentalize their existing network perimeter security by adding "Zero Trust" or "micro-segmented" network environments *within* the data center. A zero trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems and/or applications within the data center network. When a user or system "breaks the rules," the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks. Only those with the full key ring can move freely within the data center. Limiting the intruder's ability to move around freely within the house significantly mitigates the magnitude of a perimeter security breach, or break-in.

Address the Threat: Raise the Standard for Cyber Security

Cyber attacks pose a real and imminent threat to U.S. national security. Every agency needs to develop a sense of urgency and needs to be incentivized to do something beyond the status quo, because the current approach it is not working. We know the threat landscape is constantly evolving; as soon as one vulnerability is mitigated, another threat vector arises. The attackers deploy software that is being written, updated, and refined on a daily basis and this fact puts our agencies at a tactical disadvantage on a daily basis. Put simply, agencies that rely on a hardware-based perimeter security strategy cannot keep pace in a dynamically changing software-defined world.

Clearly, our nation's security posture needs to be significantly upgraded inside the network perimeter and throughout the data center. New cyber security approaches, such as Zero Trust and micro segmentation, should be adopted to enhance the government's cyber security practices. These new approaches are already the gold standard for commercial industry and need to become the gold standard across the Federal Government. VMware has implemented architectures leveraging these approaches in industries that are technology early adopters such as banking and universities. To facilitate this adoption in the federal government, policies such as FISMA should establish ratio metrics for the number of systems or workloads that a given system can access before passing though a security control. Typical agency networks have a ratio of 1 to hundreds or 1 to thousands. The target ratio should be 1 to ones or 1 to tens so that if a given network is breached, the damage will be significantly constrained. Metrics will enable Government mandates and policies (e.g. FISMA) to withstand today's cyber warfare reality.

While there is no silver bullet to permanently address every cyber security threat, Congress can mandate that agencies adopt policies and security standards that mitigate threats inside the network perimeter.

Address the Threat: Secure Existing Cyber Infrastructure

VMware supports almost every federal agency in the U.S. Government in some part of their data centers. We have seen many agencies conclude that the most effective means of mitigating the potential for a breach is to build a new network environment or data center (a "greenfield" environment) with enhanced security protocols and new perimeter or identity management based technologies such as OPM did with their "Shell." Agencies reach this conclusion because existing data centers (a "brownfield" environment) are assumed to be compromised and unsalvageable. The typical response is to stand up a new data center and methodically move workloads and applications from the old data center or brownfield environment to the new greenfield environment or data center once it is operationally ready. This is a legitimate strategy and a process that VMware supports across our customer base.

However, while the overall strategy may be legitimate, it fails to address the persistent security threat to existing cyber infrastructure. There are two main issues with this approach:

- Existing networks or data centers continue to operate while the new environment is being provisioned, which leaves sensitive data vulnerable to continuing attack. It can take months or years to stand up a new greenfield environment. As we've seen, this is what happened with the attack at OPM.
- Without clear cyber security guidelines mandating new software based security strategies that go beyond perimeter-centric security (e.g. Zero Trust or micro segmentation), the new environments are subject to attack as soon as they are operational.

In an era of constrained resources and imminent threat, this approach is insufficient and untimely. Agencies have the ability today to upgrade the security posture of their existing cyber infrastructure to and add Zero Trust software defined solutions that are inherently more cost-effective than new, expensive hardware based solutions. By deploying Zero Trust technologies within our nation's existing networks and data centers, agencies can avoid billions of dollars of additional investment in new greenfield infrastructure when the compelling driver for a greenfield investment is strictly security related.

Summary

VMware is committed to supporting the U.S. Government's efforts to defend our national cyber infrastructure. To be clear, VMware knows that every federal agency, including OPM, is aware of the persistent cyber security threat and is working diligently to address those threats on a daily basis. We applaud the government's efforts and we will continue to encourage them to adopt and deploy the Gold Standard of cyber security across all of their networks.

In our view, all U.S Government Agencies should:

1) For all existing networks, cut the common thread found in every major breach by implementing a Zero Trust security model and reducing attacker/threat mobility within the network.
2) For all new networks, change the way new cyber infrastructure is built and operated by establishing new cyber security standards and metrics that mandate a Zero Trust security model.

VMware sincerely appreciates the opportunity to share our thoughts and suggestions on this very important matter. We applaud the leadership and vision of the Chairmen and Ranking Members in holding this important joint hearing. VMware looks forward to continuing to participate in efforts to improve the security of the federal government. Thank you for the opportunity to testify today.

Martin Casado

Senior Vice President and General Manager, Networking and Security Business Unit

Martin is a VMware Fellow, and Senior Vice President and General Manager, Networking and Security Business Unit at VMware. He joined VMware in 2012, when the company acquired Nicira, of which he was co-founder and Chief Technology Officer. Martin received his PhD from Stanford University in 2007 where his dissertation work led to the creation of the software-defined networking (SDN) movement, and laid the foundation for the new paradigm of network virtualization. He received his Masters from Stanford University in 2005. While at Stanford, Martin co-founded Illuminics Systems, an IP analytics company, which was acquired by Quova Inc. in 2006. Prior to attending Stanford, Martin held a research position at Lawrence Livermore National Laboratory where he worked on network security in the information operations assurance center (IOAC). Martin has been recognized as one of the industry's leading innovators, and has been featured as one of Business Insider's "50 Most Powerful People in Enterprise Tech," *Forbes*' "Next Gen Innovators," and *Silicon Valley's Business Journal's* "Silicon Valley 40 Under 40." In 2013, Martin was also honored with the Grace Murray Hopper Award as Outstanding Young Computer Professional of the Year.

Chairwoman COMSTOCK. Thank you.

And now we will hear from Mr. Schneider.

TESTIMONY OF MR. KEN SCHNEIDER, VICE PRESIDENT OF TECHNOLOGY STRATEGY, SYMANTEC CORPORATION

Chairwoman Comstock, Chairman Loudermilk, Chairman Smith, Ranking Members Lipinski and Beyer, thank you for the opportunity to testify today.

The focus of today's hearing is right on point: Cybersecurity is a shared responsibility, and the public and private sectors must work together closely to counter ever-evolving threats.

Many of the recent headlines about cyber-attacks have focused on data breaches, both in government and across the spectrum of industries, but cyber-attacks do much more than that, and the incidents we see today range from basic confidence schemes to massive denial-of-service attacks to sophisticated and potentially destructive intrusions into critical infrastructure systems. The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, individual cyber criminals, so-called hacktivists, and state-sponsored groups. Attack methods vary, and the only constant is that the techniques are always evolving and improving. For instance, spearfishing, or customized targeted emails containing malware or malicious links, is still one of the common forms of attack. Social media is also an increasingly popular attack vector as people tend to trust links and postings that appear to come from a friend's social media feed.

We've also seen the rapid growth of targeted web-based attacks known as "watering hole attacks" and trojanized updates where malware is cloaked in legitimate software updates. For example, last year, legitimate software developers were tricked into using compromised software to publish their apps. These apps were then pushed into Apple's App Store and downloaded by unsuspecting consumers.

Further, the attack surface continues to expand as both the private and public sectors move to the cloud, and the internet of things and the billions of new devices coming online will bring them with a new generation of security challenges. For example, CCS Insight predicted the sale of 84 million wearables in 2015. Each of those 84 million users is transmitting sensitive data into cloud platforms that must be secure.

Preventing these attacks requires layered security and an integrated attack. At Symantec, we refer to this as our uniformed security strategy. The National Institute of Standards and Technology's framework for improving critical infrastructure security reflects this holistic approach and its core five functions serve as a useful outline for discussing a unified approach to security.

First is identify. Simply put, you can't protect what you can't see, but the task goes beyond just identifying hardware and software and includes a risk-based approach to ensure that the most critical assets are identified and protected.

Next is protect, and it starts with people. An organization needs to ensure that its workforce practices good cyber hygiene and is alert for the latest scams and schemes. But of course, technology is important too. Modern endpoint security examines numerous characteristics of files to discover unknown or emerging threats that might otherwise be missed. It's critical to monitor the overall operation of a system to look for unusual, unexpected, or anomalous activity that could signal an infection. Information protection is equally important. This requires a data loss prevention system that indexes, tracks, and controls the access to and movement of data across an organization.

The third function is detect. An organization needs to know what is going on inside of its systems as well as who is trying to access what and how they are trying to do so. Monitor security analytics platforms and just a whole volume of machine and user data and use advanced behavioral and reputational analytics to know whether a series of anomalies is an indicator of malicious activity. By doing so, these systems are able to detect threats that bypass other protections.

Fourth is respond. Good planning is the foundation of an effective cybersecurity strategy. If and when an incident occurs, an organization must have a well-defined and practice playbook to be able to respond quickly and effectively. Interviewing potential vendors and assigning roles and responsibility is not a good use of time while an organization is hemorrhaging sensitive data.

The last function is recover. This is twofold: getting the impacted systems back up and running, and improving security based on the lessons learned from the incident. Effective and efficient recovery requires preparation and planning. For example, poor preparation could leave an organization with incomplete or corrupted backups. But perhaps the most important part of fixing identified flaws in both systems and processes is to learn from the incident.

Cooperation is key to improving cybersecurity, and Symantec participates in numerous industry consortia and public-private partnerships to combat cyber crime. These include National Cyber Forensics and Training Alliance, FBI, Europol, Interpol, NATO, and Ameripol. We've also been involved in several operations to take down criminal networks including several high-profile botnets such as the financial fraud botnet Gameover Zeus, the ransomware network Cryptolocker, and the Ramnet botnet.

The only path to improving security for the Nation is through partnership and shared expertise, and the government can learn from the private sector's experience incorporating cutting-edge security tools into their security programs.

We appreciate the Committee's interest in learning from Symantec's expertise and best practices, and I'll be happy to take any questions. Thank you.

[The prepared statement of Mr. Schneider follows:]

Symantec.

Prepared Testimony and
Statement for the Record of

Kenneth Schneider
Vice President & Fellow
Symantec Corporation

Hearing on

"Cyber Security: What the Federal Government Can Learn from the Private Sector"

Before the

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Research and Technology
and
Subcommittee on Oversight

January 8, 2016

Chairwoman Comstock, Chairman Loudermilk, Ranking Members Lipinski and Beyer, my name is Ken Schneider. I am the Vice President of Technology Innovation at Symantec where I focus on innovation, strategic investment and aligning our security technology development vision to our strategy. I am also a Symantec Engineering Fellow, one of a select group of employees who have been recognized as Symantec's top experts in a specific field. Prior to joining Symantec, I was the Chief Technology Officer and Vice President of Operations for Brightmail, an anti-spam software company that was acquired by Symantec in 2004. Before that I founded South Beach Software, a software and consulting company that developed products for the professional video market, and also acted as an independent software consultant for clients including Sun Microsystems and Digital Equipment Corporation. I received a master of science in mechanical engineering from the University of California at Berkeley and a bachelor of science in engineering from Swarthmore College.

Symantec protects much of the world's information, and is the largest security software company in the world, with 33 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording thousands of events per second, and more than 500 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The focus of today's hearing is right on point: cybersecurity is a shared responsibility and the public and private sectors must work together closely to counter ever-evolving threats. I am excited to share my and Symantec's expertise to assist the government in improving its cybersecurity posture. In my testimony today, I will discuss:

- The current threat environment;
- An overview of how large organizations can protect themselves; and
- How we partner with the government to improve cybersecurity.

I. The Current Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on data breaches in government and across the spectrum of industries. Indeed, the recent theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches surpassed *one billion*. Yet while the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have damaging consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government.

The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary –

the criminals generally are looking for some type of financial gain, the hacktivists are seeking to promote or advance some cause, and the state actors can be engaged in espionage (traditional spycraft or economic) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Attack methods vary, and the only constant is that the techniques are always evolving and improving. Spear phishing, or customized, targeted emails containing malware or malicious links, is the most common form of attack. Many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

In addition, the attack surface continues to expand as both the private and public sectors move to the cloud. Cloud security creates new types of challenges as information is now hyper-distributed -- even tracking where your information is located is a significant problem for most large organizations. Further, the Internet of Things, or IoT, and the billions of new devices coming online, many of which create sensitive information, are posing the next generation of security challenges. And of course there are many IoT use cases that touch critical infrastructure, including transportation, smart buildings, smart cities, smart energy, etc.

Social media is an increasingly valuable tool as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to ask if that feed may have been compromised or spoofed. We have also seen the rapid growth of targeted web-based attacks, known as "watering hole" attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals lie in wait on legitimate websites that they previously compromised and use to infect visitors. Most of these attacks rely on social engineering – simply put, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

And while many assume that these attacks are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a 2015 report from the Online Trust Alliance, 90 percent of the breaches in 2014 could have been prevented if organizations implemented basic cybersecurity best practices.[1] Unfortunately, systems of all types – from the home computer to those running our nation's critical infrastructure – are similarly vulnerable. The good news is that most of these attacks can be stopped, or at worst contained, if organizations use modern security tools and best practices.

II. A Unified Approach to Security

Good security is layered security, and it requires unity of effort. At Symantec, we refer to this as our *Unified Security Strategy*. An organization cannot just throw technology or money at the problem haphazardly and hope for the best. Nor can organizations expect to remain outside the fray – attackers will find and target them, and in all likelihood will find some vulnerabilities to try to exploit. To counter this, organizations need to plan – to defend their systems, to protect their most critical data, and to respond and recover when they are attacked. It is important to recognize that the compromise of one computer or system is not the end of the story, but rather just the beginning. The efficacy of the

[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

security tools installed and the quality of the plans put in place are the key factors that will determine how successful an organization will be in thwarting an attacker.

The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Security (also known as the Cybersecurity Framework or CSF), is an excellent tool for organizations of all sizes.[2] NIST worked closely with the private sector for more than a year to develop the CSF, and the result is a document that reflects the best thinking of cyber experts from across the spectrum of security vendors and industry users. The CSF is not your traditional government document – it is not a standard, a set of controls, or a checklist. Instead, it is a tool to help organizations assess and improve their cybersecurity programs, or to build one if they do not already have one. The CSF "core" consists of five functions:

- **Identify** – understand what systems, assets, data, and capabilities need to be protected and establish processes to do so;
- **Protect** – develop and implement appropriate safeguards to critical services;
- **Detect** – develop and implement the appropriate activities to identify a cybersecurity event;
- **Respond** – develop and implement the ability to respond to a cybersecurity event; and
- **Recover** – develop the ability to restore capabilities if they are impaired by a cybersecurity event.

The CSF breaks each core function into "Categories" and then further into "Subcategories," and for each Subcategory, NIST provides a list of existing, commonly-accepted standards or practices that illustrate a method for accomplishing the designated activity. A category is a set of cybersecurity activities under a designated core function, and subcategories are tactical activities that are supposed to satisfy the programmatic needs of a given category.

Notably, the CSF is as useful for more traditional business functions as it is for security professionals; in fact, at Symantec we used the core functions of the CSF to brief our Board of Directors on our internal security posture while the CSF was still in draft form. Late last year, NIST issued a Request for Information seeking feedback on whether the CSF should be updated, and we look forward to working with NIST to evolve the CSF further.

This unified approach to security will benefit the government just as much as it will the private sector, and there are numerous private sector best practices and standards (many of which are included in the CSF) that could improve the cybersecurity of Federal agencies. So too will full implementation of cutting edge security tools, many of which are already owned by the Federal government. The government has made strides over the past few years to improve its cybersecurity posture, and the renewed focus after the OPM breach has accelerated needed improvements. It is clear that modernizing any organization's security posture, whether it be government or industry, is not a unique endeavor. As such, the government should look to those organizations with strong lessons learned, and the experts who aided them, for assistance in securing their networks.

Digging Deeper – How Organizations can Protect Themselves

Many organizations manage their own security, but even some of the country's largest companies have looked to outside experts to assist with their security programs or even to run them. For those who look for outside support, there are a several providers who can assist them, and we offer a wide range of support through our *Managed Security Services* unit. Organizations can bring in experts for everything

[2] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

from backstopping their own security programs to managing their complete day-to-day operations. But irrespective of whether an organization manages its own security or engages outside experts, the CSF provides a structure for a holistic approach to cybersecurity, and the five core functions serve as an outline for discussing a unified approach to security.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.[3]

Simply put, one cannot effectively protect what cannot be seen – this is the foundation for all security planning. But the task goes beyond just identifying hardware and software – it includes the planning that will carry throughout a security program. This is where organizations put policies in place to ensure that assets are identified and protected, to know what to do when policies are violated, and to be prepared to respond to an intrusion.

The identification has to be flexible, and a good plan will recognize that in a large enterprise it is impossible to have 100 percent awareness of every asset 100 percent of the time. Thus, the security plan and related policies need to account for this reality. The organization must have tools to assess risk and to remediate it, based on the severity. It is important to use a risk-based approach as not all assets are created equal, and not all data carries the same value. Thus, you have to put your security investments against the things that matter the most.

To accomplish these functions, there are technological solutions that can scan networks to map systems and find assets. At Symantec, we provide a tool called *IT Management Suite (ITMS)* which performs hardware and software asset discovery and management. We also have a tool known as *Control Compliance Suite (CCS)* that has a standards management module that allows an organization to conduct scans to determine whether assets are appropriately configured. CCS also contains a policy manager tool that provides an easy way to establish and update company-wide policies as well as to check compliance with those policies.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.[4]

There are numerous elements to this function, both human and technological. On the human side, an organization needs to ensure that its workforce practices good cyber hygiene, is alert for the latest scams and schemes, and understands the security policies. This is a continuing process – new staff needs to be trained, and existing employees need refreshers and updated training. An alert employee can prevent an intrusion or, if a system is already compromised, spot anomalous behavior that could allow a compromise to be contained before any damage is done.

For example, at Symantec we regularly send phishing emails to our own employees both to keep them sharp and to educate them about new and evolving phishing techniques. Individuals who are fooled by the phishing attempts are provided with a short on-line tool that educates them on how to spot them in the future. This program, known as *Symantec Phishing Readiness*, is available for our customers to use so that they too can provide training and awareness in real time.

Unfortunately, not all breaches happen because of accidental or inadvertent actions – malicious insiders pose a real and significant threat. Here technology can help, as strong identity and access management

[3] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014 at p. 8 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

[4] *Id.*

tools are key to preventing harm by malicious insiders. These tools can do more than limit data access to users with a need to know – they can do social mapping which will learn how users behave on networks and then alert managers to any unusual or outlying activity. These tools can verify that a user is who they claim to be, and that they have the correct credentials to access the system or particular data. At Symantec, we employ a variety of tools including our own *Validation and ID Protection service (VIP)* and our *Identity Access Manager*.

Identity verification is essential for all users, and user authentication is a core component of our unified security approach. VIP and Identity Access Manager fill that role for us. We are well past the days when a password, even a complex one, will be much more than a speed bump for a sophisticated attacker. Multi-factor authentication – combining something you know (such as a password) with something you have (such as an authentication token or mobile application) – is essential for any system to be secure. Many of the recent high profile breaches would have been prevented had the victims employed multi-factor authentication. A good access manager can also minimize the number of passwords employees need to keep, as it can serve as a portal to myriad tools after the user is properly authenticated.

To combat ever-evolving threats, organizations need to protect both their systems and their data. Perimeter security such as a firewall that scans incoming and outgoing traffic is one piece of the puzzle, but it is just a start. Most intrusions begin on a single compromised device which the attacker uses to establish a beachhead. To counter this, modern endpoint security will do two things that go far beyond the simple antivirus of the past. First, it will look at the age, frequency, location and other characteristics of any file that tries to execute on a computer to expose unknown or emerging threats that might otherwise be missed. For example, if a computer is trying to execute a file that the security system has never seen anywhere in the world and that comes from an unknown source, there is a high probability that it is malicious. Second, it will monitor the overall operation of the system to look for unusual, unexpected, or anomalous activity that could signal an infection. At Symantec, we refer to this as reputation-based security that looks holistically at numerous factors associated with digital files to determine how safe it may be on the security spectrum. We do this through tools such as *Symantec Endpoint Protection* and *Data Center Security*.

Data protection is equally important, and a comprehensive security plan tackles data protection with tools that are distinct from those designed to prevent intrusions. A good data loss prevention (DLP) system will index, track, and control the access to and movement of even huge volumes of data across an organization, and most importantly will prevent data from moving outside an organization. Organizations also should use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key. Finally, as part of a risk based approach, after identifying the most valuable data – the so-called "crown jewels" – one needs to apply appropriate protections, which can include virtually or physically isolating a system, applying additional access controls to it, and more. Symantec is a provider of *Endpoint Encryption*, as well as *Data Loss Prevention (DLP)* software, which is an industry leading tool that allows organizations to tailor these controls to their specific needs.

Organizations should also look at any characteristics peculiar to their operation and determine if there are additional protections available that will make it harder for an attacker. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. Symantec's *Critical System Protection (CSP)* is highly effective at preventing the theft of credit card and other personal information from these systems because it does not allow unknown or malicious code to execute on the device. In the critical infrastructure sectors, CSP can assist operators to ensure that the systems that control machinery and other critical systems are hardened and isolated to prevent an attacker from being able to reach them, even if the organization's business systems were compromised.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.[5]

In the simplest of terms, an organization needs to know what is going on inside of its systems – as well as who is trying to access it and how they are trying to do so. Good security means looking for anomalous behavior that could indicate the presence of a new threat or a previously unknown attack. Modern security suites will look at the connections that your system is making to see if a machine is talking to a known bad actor or to a suspicious domain; they will look for activity that is outside the normal behavior for a given machine; and they will flag unusual transfers of data, whether within a system or to someone outside of it. But detection goes beyond monitoring what the machines are doing – it is equally important to assess authorized user activity to look for both accidental and intentional violations of security policies. This can include transferring a business file to a personal device to work on at home or a large scale theft of company data.

Analytics such as these are perhaps the fastest evolving area in cybersecurity. Modern security suites ingest a huge volume of machine and user data and, using rules set by the organization, develop a profile of what is normal and allowed for a given system or user. These systems learn continuously, and alert when a rule or policy is violated. The key to doing this effectively is identifying what to look for – a system is only as smart as the rules that govern it and the data it has to analyze. The latest evolution in this approach is systems that draw inferences from seemingly unconnected bits of data and, using advanced behavioral and reputation analytics, know that a series of anomalies could be an indicator of malicious activity. By doing so, these systems are able to detect threats that bypass other protections.

At Symantec, we refer to this as our *Unified Security Analytics Platform*. It derives information from Symantec protected endpoints, data centers, and gateways and incorporates log and telemetry files, behavioral, reputation, and threat analytics, global threat intelligence, and actionable insights to provide the key inferences to connect the dots. We use this to protect our own networks and those of our customers worldwide.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.[6]

Good planning is the foundation of an effective response, and studies have shown that organizations that prepare in advance minimize the damage of a breach and expend fewer resources when an incident occurs.[7] Planning is both a human and a machine exercise. It is up to an organization's leaders to stress the importance of preparation and to lead the effort, and key responders need to be identified and trained ahead of time. Indeed, everyone involved in the response should know his or her roles and responsibilities before an event happens.

It is also useful to identify ahead of time any outside expertise that may be needed to contain a major incident. Interviewing potential responders is not a good use of an organization's time while it is hemorrhaging sensitive data, and the middle of a crisis is rarely the best time to make decisions about outside vendors. It also is useful to establish relationships with law enforcement before an attack so that you know who to call should an incident occur. Hours spent determining who is the appropriate agency to contact could be additional hours that an attacker is on your system. Moreover, should an incident escalate to the point that law enforcement is involved, it will likely be necessary to take steps to preserve log files and other data as forensic evidence – and pre-planning will help to ensure that this

[5] *Id.*

[6] *Id.*

[7] 2015 Cost of Data Breach Study: A Global Analysis, Ponemon Institute LLC, May 2015 at p. 13 (http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF?)

happens effectively. At Symantec, we have a unit called *Cyber Security Services* that can help organizations prepare for and respond to breaches.

A good planning process will necessarily lead to implementation of better security practices and tools – and will streamline the response process and limit the damage an organization will suffer. Finally, a plan needs to be exercised, both to train employees and to identify areas for improvement. At Symantec, we conduct simulation exercises (our internal "Cyber War Games") that provide hands-on training for our employees. This proved to be such a success that we developed a commercial version of it, and offer *Security Simulations* that our customers can use to train their own employees. These simulations provide a controlled environment for defenders to think like the bad guy – which in turn makes them better at protecting their systems.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.[8]

Recovery is two-fold – getting the impacted systems back up and running, and improving security based on the lessons learned from the incident. Resilience in both systems and data is essential; an organization needs clean computers and clean back-ups as recovering from a major incident will frequently involve taking systems offline, reimaging them, and restoring data. Thus, effective and efficient recovery requires preparation and planning. Making decisions and hiring vendors or consultants on the fly after an incident will certainly increase the time to get back up and very likely raise the cost of doing so. And poor preparation could leave an organization with incomplete or corrupted backups, making recovery all the more difficult.

But perhaps the hardest part is ensuring that an organization has an effective feedback loop – the ability to fix identified flaws in both systems and processes. Much of this will happen after an incident is resolved, and too often organizations are either too busy getting back up to speed or too exhausted from the event to do a thorough after-action review. Nevertheless, the immediate aftermath of the event is the best time to implement security improvements, update response plans, and consider new policies and procedures.

For example, our Global Security Office, led by our Chief Information Security Officer who is responsible for Symantec's cyber and physical corporate security, has a planning team dedicated solely to responding and recovering. They manage the planning process and any feedback loops for improvement. This plan is integrated to include all components of the response and recovery effort, including products, technology response, sales, legal, public relations, and more. The plan is reviewed regularly with the components and exercised throughout the year.

III. Partnering with the Government to Improve Cybersecurity

Symantec views our role in combating global cyber threats as a core value for the company. As such, we participate in numerous industry consortia, as well as public-private partnerships with all levels of government, both here in the U.S. and abroad. We share high-level cybercrime and cyber threat trends and information on a voluntary basis through different fora to help protect our customers and their networks. Effective sharing of actionable information among the private sector, and between the public and private sectors, on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity and deterring cybercrime. Of course, all of this work is done in keeping with both our strict privacy policies, and all applicable privacy and data protection laws.

[8] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014 at p. 8 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

Among the public-private partnerships Symantec participates in are the National Cyber-Forensics and Training Alliance (NCFTA), FBI, EUROPOL, INTERPOL, the North Atlantic Treaty Organization (NATO), and AMERIPOL. The NCFTA demonstrates how private industry and law enforcement partnerships can yield real world success. Based in Pittsburgh, the NCFTA includes more than 80 industry partners – from financial services and telecommunications to manufacturing and health care – working with federal and international partners to provide real-time cyber threat intelligence to identify threats and actors. In turn, the NCFTA provides intelligence to domestic and international law enforcement to counter those threats. Through this partnership, hundreds of criminal investigations have been launched, which otherwise would not have been addressed, with successful prosecutions of more than 300 cyber criminals worldwide. In further support of these initiatives, the NCFTA has produced more than 400 cyber threat intelligence reports over the past three years alone. Through the NCFTA, industry is able to share crucial cyber threat information across a broad group of private industry and law enforcement entities at home and abroad. [9]

Symantec also maintains relationships in the U.S. and around the world with international cyber response organizations and law enforcement entities including the FBI, INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces, by sharing the latest technological trends, the evolution of the threat landscape, and the techniques that cyber criminals use to launch attacks.

For example, in June of 2014, Symantec, the FBI, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet *Gameover Zeus* and the ransomware network *Cryptolocker*. *Gameover Zeus* was the largest financial fraud botnet in operation that year and is often described as one of the most technically sophisticated variants of the ubiquitous *Zeus* malware. Symantec provided technical insights into the operation and impact of both *Gameover Zeus* and *Cryptolocker*, and worked with a broad industry coalition and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.[10]

In February of 2015, Symantec and other industry players partnered with EUROPOL in an operation against the *Ramnit* botnet and seized its servers and infrastructure. *Ramnit* harvested banking credentials and other personal credentials from their victims. The group was in operation for at least five years and had evolved into a major criminal operation, infecting more than 3.2 million computers.[11]

Symantec also works closely with INTERPOL. In November of 2015, Symantec was invited to present at INTERPOL's Africa Cybercrime Working Group meeting held in Kigali, Rwanda. The event provided a rare forum for law enforcement cybercrime units from 13 African countries and several industry partners to exchange threat information and discuss cross-border cybercrime challenges in Africa.

In December of 2015, Symantec signed a partnership agreement with NATO's Communications and Information (NCI) Agency. NATO recognizes the importance of working with industry to address emerging cybersecurity challenges that may affect the ability of NATO to achieve its mission of defending its member nations. A number of activities are already underway, including sharing cyber threat information, capacity building and promoting technological innovation to address emerging challenges.[12]

[9] https://www.ncfta.net/about-ncfta.aspx

[10] http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

[11] http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

[12] https://www.ncia.nato.int/NewsRoom/Pages/151211_NATO-builds-cyber-alliances.aspx

Symantec also has partnered with AMERIPOL and the Organization of American States to publish a report in June of 2014 that provided the most comprehensive snapshot to date of cybersecurity threats in the Latin American and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as national and economic security imperatives. Similarly, Symantec is partnering with the African Union and the United States Department of State Office of the Cyber Coordinator to develop a report examining the cybersecurity threats and trends in Africa. That report will be published later this year.

Private to private partnerships have also proven to be effective in fighting cybercrime. An excellent example of the private sector banding together is the establishment of the Cyber Threat Alliance (CTA). The CTA is a group of cyber security practitioners from Symantec, Intel Security, Palo Alto Networks and other firms that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member companies and their customers. By sharing detailed security information we can improve overall protection for our customers – many of whom use multiple security products. The bulk of information sharing before the CTA was established primarily involved sharing malware samples. The CTA builds upon this foundation by sharing more actionable threat intelligence, including information on zero day vulnerabilities, botnet command and control server information, mobile threats, and indicators of compromise related to advanced persistent threats, to combat more advanced attacks. [13]

Conclusion

Cybersecurity is not the sole province of the government or the private sector; the only path to improving security for the Nation is through partnership and shared expertise. The NIST CSF – itself the result of a successful collaborative public-private effort – is a tool that can be used to build out a cybersecurity program or to assess an existing one. It is equally useful to Federal agencies, which can use it to assess their own security posture as well as look to private sector experience with the CSF in order to maximize its utility. Similarly, the government can look to the private sector's experience incorporating cutting edge security tools into their security programs. Simply put, good standards and policies in combination with tools like data loss prevention, endpoint security, strong firewalls, security analytics, and multi-factor authentication are the building blocks of a good cybersecurity program.

We appreciate the Committees' interest in learning from Symantec's expertise and best practices, and we look forward to continuing to partner in the future.

[13] http://cyberthreatalliance.org/mission.html

Chairwoman COMSTOCK. Thank you.

And now we'll hear from Mr. Clinton.

TESTIMONY OF MR. LARRY CLINTON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET SECURITY ALLIANCE

Mr. CLINTON. Thank you, Madam Chair and Members of the Committee. It's an honor to be here. I appreciate the opportunity.

I'd like to focus on five areas I think where the federal government can learn from the private sector. First, government needs to invest much more in cybersecurity. Private-sector spending on cybersecurity has nearly doubled in the last several years to $120 billion annually. The federal non-defense spending on cybersecurity this year will be between $6 and $7 billion. Private-sector spending on cybersecurity will increase 24 percent next year. Federal government spending is increasing about 11 percent. I know of two banks who have a combined cybersecurity budget of $1.25 billion for next year. DHS's entire budget for cybersecurity next year is about $900 million, 75 percent of what two banks are spending by themselves. Cyber crime costs our nation a half trillion dollars a year, yet we are successfully prosecuting maybe one percent of cyber criminals. We simply need to spend more on cybersecurity.

Two, government needs to act with greater urgency. It took Congress six years to pass a modest information-sharing bill. In 2009, major trade associations presented Congress and the Administration detailed recommendations on cybersecurity. In 2011, the House GOP task force report on cybersecurity embraced these recommendations, as did President Obama's Executive Order, but four years after the House task force report, we still have not seen any substantial work on the top recommendation in that report or the Executive Orders. For example, the GAO task force report and the Executive Order and the national infrastructure protection plan all call for the creation of a menu of incentives to promote the adoption of cybersecurity yet aside from the information-sharing bill, the President has not proposed, Congress has not introduced a single incentive strategy bill. Last month GAO reported that 12 of 15 sector-specific agencies had not identified incentives to promote cybersecurity even though that's called for in the national infrastructure protection plan. The President's Executive Order called for the NIST cybersecurity framework to be both cost-effective and prioritized. Three years later, there has been no objective measurement of the framework's effect on improving security, adoption or its cost-effectiveness.

Three: The government needs to educate top leadership as the private sector is doing. In 2014, ISA and AIG created handbook on cybersecurity for corporate boards, which was published by the National Association of Corporate Directors and is the heart of the training program that they are launching. PriceWaterhouseCoopers recently validated the success of this approach. They said boards appear to be listening to the NACD guidance. This year we saw a double-digit increase in board participation in cybersecurity leading to a 24 percent boost in security spending. Other notable outcomes include the identification of key risks, fostering an organizational culture of security, and better alignment of security with overall risk management and business goals.

We believe, Madam Chair, that the government needs a similar program to educate the government equivalence of corporate boards: Members of Congress, members of the Cabinet, agency Secretaries. Most senior government officials are not sophisticated with their understanding of cybersecurity. If they are educated as we're educating the private sector, we think we could have more effective policy.

Four: The government needs to reorganize for the digital age. Over the past several years, the private sector has moved away from the IT department as the central focus of cybersecurity and is evolving a more integrated enterprise-wide risk management approach. Unfortunately, the federal government is still caught up in legacy structure and turf wars that are impeding our efforts. A Bank of America/Merrill Lynch study found in 2015 that the U.S. government is still in the process of determining who will have jurisdiction in cyberspace. Departments, agencies, and commands are all battling for jurisdiction and funding. The result is a fragmented system, muddled political agendas that is hindering the development of a secure system.

And finally, five: Government needs to become more sophisticated in managing their own cybersecurity programs. A 2015 study compared federal civilian agencies with the private sector, and found that the federal agencies ranked dead last in terms of understanding cybersecurity, fixing software problems, and failed to comply with industry standards 75 percent of the time. The reason the government does so badly, according to GAO, is that they simply evaluate by a predetermined checklist. The private sector, on the other hand, uses a risk management approach wherein we anticipate what the future attacks are going to be based on our risk posture and then forward looking attempt to adopt standards and practices.

We believe that the government needs to follow the private sector's lead. They need to become more educated, more sophisticated, and more innovative and act with greater emergency and commitment with respect to cybersecurity.

I appreciate the opportunity to speak to you today. Thank you.

[The prepared statement of Mr. Clinton follows:]

TESTIMONY

LARRY CLINTON
PRESIDENT, INTERNET SECURITY ALLIANCE

WHAT GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR ON CYBER SECURITY

JANUARY 8, 2016

Mr. Chairman let me put this simply. We are not doing enough to combat the growing cyber threat, and what we are doing we are not doing nearly fast enough.

THE NEED FOR US TO WORK BETTER TOGETHER

The core question of today's hearing -- what can the public sector learn from the private sector -- is an excellent question.

Not only **can** we learn from each other, we **need** to learn from each other. Moreover, we need to be working together much more effectively

AT LEAST WE ARE ON THE RIGHT PATH -- JUST MOVING TOO SLOWLY

To be fair there has been progress -- learning -- at least at the broad policy level. Just a few years ago both Republicans and Democrats were offering legislative proposals on cyber security that basically tried to adapt a traditional regulatory model to the cyber problem as if we were dealing with a simple consumer product safety issue that could be solved. That approach would have failed miserably.

In 2009 the ISA produced the "Cyber Security Social Contract"[1] that described why the traditional regulatory model not only wouldn't work, but would be counter- productive to enhancing our security and offered a different approach. The Social Contract model proposed that government and industry work together to identify effective standards and practices and that voluntary adoption of these standards and practices ought to be motivated via a system of incentives.

In 2011 a broad spectrum of the private sector including the ISA, US Chamber of Commerce, Tech America, the Business Software Alliance and the Center for Democracy

[1] http://isalliance.org/publications/2B.%20Social%20Contract%202.0%20-%20A%2021st%20Century%20Program%20for%20Effective%20Cyber%20Security%20-%20ISA%202010.pdf

and Technology embraced the social contract approach in a comprehensive whitepaper on cyber security.[2]

In 2012 the House GOP Cyber Security Task Force appointed by Speaker Boehner and Chaired by Mac Thornberry listened as all 5 private sector organizations supported this model and in the end the GOP Task Force endorsed this approach. [3]

In 2013 President Obama, reversed his earlier government centric regulatory approach and also listened to the private sector. He then issued Executive Order 13636 on cyber security[4] which similarly embraced the Social Contract approach and directed the National Institute on Standards and Technology (NIST) to develop the framework of cyber standards and practices and directed federal agencies to determine what incentives could be offered to promote voluntary adoption of the NIST Framework.

The recently enacted information sharing legislation is an example of this approach. It does not mandate information sharing with the government -- as for example does the current EU proposal does -- but motivates voluntary sharing by offering a liability incentive. This approach has received bi-partisan support in the Senate and is supported at least conceptually by the Administration.

A related example of the federal government listening to the private sector with respect to information sharing has to do with the information sharing mechanisms and their need of reform. Again harkening back to the ISA's 2009 Cyber Social Contract document and the subsequent multi-trade association white paper of 2011, the private sector argued that the historic sector-by-sector structures of information sharing were inadequate and inefficient.

From a cyber security perspective large defense contractors probably have more in common with large financial institutions than with small banks and "mom and pop" component suppliers within their so-called sectors. More importantly, the existing structures were primarily attuned to the needs and processes of larger institutions leaving small and mid-sized players largely as non-participants in information sharing programs. A far more effective structure would be cross-sector information sharing especially among the major players with economies of scope and scale who could then manage the sophisticated information they can generate and analyze amongst themselves and pre-digest it into actionable elements for smaller players.

[2] http://isalliance.org/publications/2C.%20Industry-Civil%20Liberties%20Community%20Cybersecurity%20White%20Paper%20-%20Improving%20our%20Nation's%20Cybersecurity%20through%20the%20Public-Private%20Partnership%20-%203-2011.pdf

[3] http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf

[4] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Once again the government has listened. In February of this year President Obama signed Executive Order 13691[5] that seeks to expand the current "ISAC" model and spur the development of broader "ISAOs" many of which will operate across the sectors and specifically design programs to make cyber information shared more timely, digestible and actionable for the smaller organizations who we now understand are not only targets in their own right but conduits to larger elements of the critical infrastructure. DHS has initiated a grant process to establish a standards organization to facilitate the development of these new, more modern information-sharing entities.

These positive steps to enhance our nation's cyber security are an outgrowth of the policy makers listening to and learning from the private sector, which has greater experience with, and understanding of, the cyber security problem.

This listening model needs to be followed and expanded and we congratulate the Committee for being supportive of that effort.

10 LESSONS THE GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR

1. The government needs to invest more on cyber security.

For the past two years, the United States Worldwide Threat Assessment has listed cyber-attacks above all other threats to US national security – including terrorist and nuclear threats from the middle-east[6]. Director of National Intelligence James Clapper has told Congress "We must be prepared for a catastrophic large-scale cyber strike. We've been living with a constant and expanding barrage of cyberattacks for some time. This insidious trend will continue. Cyber poses a very complex set of threats, because profit- motivated criminals, ideologically motivated hackers, or extremists in variously capable nation-states, like Russia, China, North Korea, and Iran, are all potential adversaries, who, if they choose, can do great harm.[2] Likewise, a recent survey of worldwide stakeholders from the financial services industry ranked cyber risk as by far the single biggest risk to broader global economy.[7]

While the cyber threat to the United States continues to increase in severity and scale of impact, a disparity exists between federal and private sector spending on the issue.

[5] https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[6] http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1175-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee

[7] http://dtcc.com/~/media/Files/pdfs/Systemic-Risk-Report-2015-Q1.pdf

According to the Ponemon Institute, total private sector spending on cyber security (not just IT) has doubled in the past few years and now exceeds $100 billion annually. Federal spending on cyber security is about $13 billion and nearly half of that goes to the military that is largely offensive oriented cyber programs, which, while vital, are not security in the sense we are discussing it today.

That leaves about 6-7 billion dollars a year to fight a problem that experts estimate is costing us many hundreds of billions of dollars, maybe a trillion dollars a year in lost value of IP, business practices and data ---leaving aside the national security risks engendered by private sector losses through cyber means.

I know of two banks that have a combined cyber security budget of $1.25 billion. The DHS cyber budget ---to manage securing the entire civilian government and critical infrastructure is about 900 million ---75% of what just two banks spend.

Meanwhile, the US is spending $95 Billion dollars a year combatting terrorist threats in the middle-east[8] The US spends around $52 Billion dollars[9] a year on our nuclear weapons program and $15.5 Billion a year on securing our southern border[10]

To use Department of Homeland Security spending as a reference, barely 2% ($1.25 Billion) of DHS total 61 Billion dollar budget allocation for fiscal year 2015 is dedicated to cybersecurity activities. DHS spends nearly $6 Billion on immigration issues and $7 Billion is allocated to TSA respectively.

No one is saying these expenditures are not important. However, if our own threat assessment says cyber is the number one threat costing us hundreds of billions of dollars a year, threatening the economic vitality and personal privacy of millions of Americans every day and potentially threatening our national security --- is it logical that our spending on it should be less than half what we are spending on the southern border and one tenth of what we are spending on nuclear which our own official threat assessments rate currently as lower risks? [11]

While the percentage increases in federal cyber spending may sound impressive ---up 35% in the last 3 years ---they are perhaps misleading due meager baseline spending up until very recently. The absolute dollar amount being spent on cyber security in relation to the size of the problem is nowhere near adequate.

[8] http://fas.org/sgp/crs/natsec/RL33110.pdf

[9] http://carnegieendowment.org/2009/01/12/nuclear-security-spending-assessing-costs-examining-priorities/8uq

[10] http://www.cbp.gov/sites/default/files/documents/FY2013%20Summary%20of%20Performance%20and%20Financial%20Information%20-%20FINAL%20%28panels%29%20%20%20.pdf

[11] http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf

Pricewaterhouse predicts privet sector spending on cyber security will increase 24% this year. Federal spending is going up roughly 10% a year.

Cybercrime costs our nation about a half trillion dollars a year. Yet we successfully prosecute about 1% of cyber criminals.

The spending on cyber law enforcement is an excellent example. Multiple independent studies have concluded that the financial losses being suffered by American citizens and businesses -- often at the hands of nation-state affiliated attackers who are using cyber attacks to prop up their domestic economies -- runs to the hundreds of billions of dollars each year.

Yet we are spending maybe one tenth of one percent of that amount to capture these criminals. Our valiant law enforcement officers are fighting the good fight but are hopelessly out matched in terms of overall resources and personnel ---and the attack community is investing at a much higher rate than we are on the law enforcement side where we are fighting to achieve incremental operational increases.

2. The Government must act with much greater urgency on the policy recommendations it claims to have learned from the private sector

While we are naturally pleased to see the number of hearings Congress is now holding on cyber security issues, the fact remains that it took Congress 6 years to pass a fairly modest information sharing bill.

The House GOP Task Force on Cyber Security made its legislative recommendations including first and foremost the need for Congress to develop a "menu of incentives" to promote a voluntary program of cyber security in 2012. Now more than three years later, apart from the information sharing bill, there is not a single bill I am aware of in the House that follows through on that primary recommendation. Moreover, I'm unaware of a single hearing that has focused on the development of an incentive model for cyber security or even the overall economics of the cyber security issue.

Similarly the President's Executive Order on cyber security was issued in February of 2012. Yet despite some blogging by the White House there has not been a single legislative proposal come forth from the Administration following through on the President's Order to develop a set of incentives to promote voluntary adoption of the NIST Framework.

ISA alone has testified in the House and Senate more than a dozen times over its 15 year history urging that Congress enact meaningful cyber legislation and including a nearly a dozen specific incentive models. The Partnership for Critical Infrastructure Security (PCIS) participating all 18 critical sectors put forth a separate set of recommendations to the DHS at a conference specifically designed for this purpose, yet we have seen no legislative or Administrative action.

We need the government to listen to this plea

The cyber security problem is far, far, more dire than the highly publicized breaches of personal data -- horrible as they are—and things are getting rapidly worse.

Our cyber systems are getting technologically weaker as the attack community finds new weakness in the Internet's core protocols. As we vastly expand the number of access points to penetrate the system and the attack community is growing increasingly sophisticated as the elite techniques against governments and the military that we used to call the advanced persistent threat is now the Average Persistent Threat being used throughout the economy?

Congress is not moving nearly fast enough to keep up with an expanding threat to our cyber infrastructure that is moving ahead at light speed...

3. Federal Government should educate its top leadership on cyber as the private sector is doing

According to the most recent research, cyber security is now the top concern of corporate boards of directors, surpassing last year's number one issue---leadership succession. It's unknown in how many congressional offices cyber security ranks ahead of leadership succession.

Recognizing the ascendency of cyber security as an issue for corporate boards last year the National Association of Corporate Directors (NACD) asked the ISA and AIG to develop for them the first ever handbook on cyber security for corporate boards.[12]

This publication, which has subsequently been endorsed by DHS and the Institute for International Auditing and many others stresses that cyber security much be understood in a much broader context than simply breach prevention and response. Much like legal and finance considerations there is not a single major business decision before corporate boards that doesn't have a cyber security element to it.

Recently, PWC independently validated the success of this approach, in its 2016 threat landscape report:

[9] http://www.isalliance.org/national-association-of-corporate-directors-asks-isa-to-create-best-practices-guide-for-corporate-board-of-directors/

"Boards appear to be listening to the NACD guidance. This year we saw a double-digit uptick in Board participation in information security. Leading to a 24% boost in security spending... Other notable outcomes include identification of key risks, fostering an organizational culture of security and better alignment of cyber security with overall risk management and business goals."

NACD and ISA are now designing full training programs for boards, irrespective of their specific businesses, to understand and appreciate this new reality. Boards are being trained to address cyber as part of the core mission of their business and not relegate it simply to the IT department. Senior leadership must embrace this more comprehensive understanding of the cyber threats practice and instill a culture of security throughout the organization.

The federal government might do well to emulate this approach to cyber security realizing that the single greatest cyber vulnerability is not technical but human. Many in senior government leadership positions are what are often referred to as "digital immigrants" meaning they were not born into the digital world they now inhabit. As we are doing with corporate board's senior government officials may do well to be trained not just to be aware of the cyber threat, but to understand it better.

Many of the common "knowledge" and understandings about cyber security widely accepted by government officials are in fact fallacious. For example it's widely assumed that with public awareness of cyber events the stock market will penalize the companies providing a natural incentive for better security. Policy makers may be surprised to find that in reality the stock prices for such well known victim companies as Target and Sony have soured after their breaches ---an effect that has accompanied many recent high-profile breaches.

Similarly government officials have often spoken of how good cyber security is a partner to profitability. Official government publications ranging from the national Strategy to Secure Cyber Space to DHS's highly promoted "Cyber Security Eco-System" program of a couple of years ago asserted claim. The reality is that many if not most of the technological enhancements that drive productivity, growth, profitability and innovation --- VOIP, cloud computing, BYOD (Bring Your Own Device to work) actually come with substantial security downsides and mitigating these security issues comes at potentially substantial economic cost.

The point being that creating an economically sustainable secure cyber system is not easy and not necessarily pro-economic. Policy makers may benefit from the sorts of structured training programs corporate boards are undergoing to learn how best to manage this enormous risk.

Once government, like corporate, leadership better appreciate the cyber threat they will be in a better condition to make sound policy decisions and just as importantly behave in a way that models good security. Leadership needs to establish clear lines of authority and responsibility and focus on fundamentals as a foundation for all success. Deploying technology solution on top of a weak foundation will not solve problems, it will create them.

It is not required that Agency leadership become technical cyber experts, however as with the private sector, Agency leadership must realize that in the modern world much, if not all, of their missions have a cyber security component As a result, Agency leaders need to at least be able to ask the proper questions of their staff to assess how well the Agency is managing cyber risk. In this regard many of the tools the private secto4r has developed for its own senior leadership are probably easily adapted to the Agency context.

For example the Cyber Security Handbook for Corporate boards [13] ISA wrote for the National Association of Corporate Directors, provides a set of core principles for senior management to use as well as a variety of basic questions that management can ask to assess issues cyber situational awareness, strategy and operations, and incident response.

One technique a "Cybersecurity Balance Sheet" that identifies, at a high level, the company's cyber assets and liabilities and can provide a scorecard for thinking through management progress in implementing the security system.

Assessing the asset side of the balance sheet might begin with identifying the organization's "crown jewels." This is an important exercise, as it is simply not cost-efficient to protect all data at the maximum level. However the organization's most valued data, be it intellectual property, consumer or client information, financial data etc. needs to be identified. Other corporate data can be similarly categorized as to its relative security needs.

The next step is to discuss the strategy for securing data at each level. This strategy generally involves a consideration of people, process and technology.

At the technology process level there are a range of options available with good research indicating cost-effective methods to secure lower-level data and thus reserve deployment of more sophisticated—and hence costly—measures for the data of higher value.

At the people level it is important to follow leading practices for managing personnel, especially with respect to hiring, in-company moves and departures, and the associated system access permissions. Ongoing cybersecurity training is similarly important, and

[13] http://www.isalliance.org/national-association-of-corporate-directors-asks-isa-to-create-best-practices-guide-for-corporate-board-of-directors/

will be most effective if cybersecurity metrics are fully integrated into employee evaluation and compensation methods.

Of special attention is the inclusion of senior and other executive level personnel who are both highly valued targets and often uniquely lax in following through on security protocols.

Turning to the liability side of the cyber "balance sheet," an evaluation could start with a look at the business practices that might create liabilities.

Some obvious risks are created by practices such as purchasing services for an un-trusted vendor and not being conscientious regarding discontinuing access rights promptly at project or employee termination. However, additional liabilities are created more subtly from practices such the explosion of mobile devices carrying corporate data, expanding Internet functionality into nonconventional products (the so called "Internet of Things") or the unmanaged data sprawl ---and accompanying vulnerabilities-- that can be a natural byproduct of the increasingly connected world.

4. Government needs to reorganize for the digital age.

The private sector has increasingly moved away from the model wherein one particular department, typically IT, would have "ownership" over cyber security and more toward an enterprise wide model with multiple departments working together with an independent budget.

Government on the other hand has refused to break through the turf wars that are impeding progress and creating unwanted redundancies which are sapping scarce security resources.

The federal government, including Congress, is burdened with legacy structures and procedures designed for a much slower analogue world. The federal procurement systems are a prime example of this dated process. Virtually every single item the government wants to buy has to be bid on and go through an elaborate approval and procurement process. Not only are these policies cumbersome and time consuming but they are expensive as well. While private companies can quickly acquire what they need to secure their networks government agencies are bound by miles of red tape.
A 2015 study compared civilian federal agencies to the private sector and found the federal agencies ranked dead last in fixing security problems and failed to comply with security standards 76% of the time.

Similarly a slow and ineffective government hiring process drives away the candidates. The Partnership for Public Service report cited earlier also found that "the drawn out security clearance process is an impediment as in some cases recruits opt to seek employment opportunities with private industry rather than wait for the long government process to be completed.." [14]

Several of these issues were also outlined in the GAO's 2011 report, but years later the same issues remain.

A Bank of America Merrill Lynch 2015 report stated:

"The US government is still in the process of determining who will have jurisdiction in cyber space. Departments Agencies and Commands are still battling for jurisdiction and funding. The result is a fragmented system muddled with a political agenda which hinders the development of a more secure system."

The problem is not confined to the federal level either. Virtually every state states and many localities are deciding they want to have their own piece of the cyber security turf and thus are enacting unique rules restrictions and regulations. This patchwork of governmental initiatives further depletes private resources without any perceptible improvement to overall security.

5 Government needs to adopt a risk management approach to cyber security

A study published last summer analyzed the audits of software applications and vulnerabilities in the public and private sector over the past 18 months. The study found that civilian federal agencies rank dead last in fixing security problems in the software they build and buy.

The study also examined software security flaws and how often users complied with widely accepted security standards and how often the vulnerabilities were fixed.
The study found that overall federal agencies comply with widely held security standards only 24 percent of the time. By comparison the financial services industry rate of compliance was nearly double (42 percent).

The study also measured how often and how quickly software security flaws are fixed after they are found. Government agencies ranked dead last again. The study found that federal agencies patched flaws in their software only 27 percent of the time. In comparison the manufacturing sector ---not generally considered an industry leader in cyber security---fixed their flaws 81 percent of the time.

The reason government does so badly according to the GAO is that government uses a "policy based" approach where agencies check off a list of requirements set by law makers and regulators.

[14] http://ourpublicservice.org/publications/download.php?id=504

Auditors and management can look at a checklist of controls and feel good about meeting 120 out of 125 controls. But meeting standards is a measure of investment and policy decisions, not a measure of security effectiveness. At best it is an indirect indicator. It tells you if you have a firm foundation to build on, but does not tell you how well you've built on it.

The prevailing notion in Congress, government agencies, insurance companies, auditors are that all we need to do is follow the standards. It's understandable given the dearth of other comforting measurements in the cyber arena but it is, nevertheless, a dangerous notion. Standards are great to use as a checklist to ensure you haven't forgotten any of the basics, but standards adherence does not equal security. In the end, standards are about what you do, not how well you do it. What will make the difference are the operational processes and staffing that are built around the systems, which implement the standards.

When we make our primary measure of security success a checklist against standards, the result is often investment without commitment. An agency will invest in products that technically meet some aspect of a standard (typically NIST 800-53 or ISO 270001) but fail to staff it with the operational and sustaining labor needed to really take advantage of the security improvements the product will yield.

For example, agencies can meet several NIST 800-53 controls by having firewalls in place. But who is watching the firewall and looking for gaps or inefficiencies? What governance is placed around the privileged functions in a company that "need" to be outside a firewall to get the job done? Who looks at the firewall logs and thinks, "Hmmm. That looks odd. I think I better dig into that some more."

Private companies typically do the same thing but they add to their mix a risk-based approach. With a risk based approach you don't focus just on the predetermined technical check list but also analyze at what the attackers might want due to current threat indicators and what's in place to stop them. Both approaches are valid but everyone should do both. Federal agencies mostly just do the checklist.

Although government officials often talk about using a risk management approach to cyber security, the hard data demonstrates that they are not in fact following the forward looking process typically practices in the private sector, much to the detriment of the government's own systems.

6. Government does not adequately assess their cyber security programs.

ISA has been involved in numerous partnership programs with the federal government dating back to before DHS was even born. We participate in multiple Sector Coordinating Councils, We are members of DHS's Cross Sector Cyber Security Working

Group, and I have served multiple terms on the board of the Partnership for Critical Infrastructure Protection and many others. Never once has any federal official reported to us regarding the cost effectiveness of any federal partnership program.

Since NIST is in the jurisdiction of the Science Committee we can use it as an example. In 2012 President Obama charged NIST to develop a cyber security Framework. The President's order specified that the Framework be prioritized, cost effective, flexible and be supported by an incentive structure.

Many of us in the private sector praised the design process for the Framework. But once it was designed the federal government went immediately into wide-scale promotion. No sophisticated private sector entity would design a new product or service and go directly to marketing. You design, and then beta test your product or service with your target audience. Based on your beta test you make modifications and then, only then you promote the product or service.

The government simply skipped over these critical steps. As a result now, two years after the Framework was designed, we don't have a single piece of objective data that can tell us what in the Framework has changed behavior or what impact any behavior changes may have had on improving security.

As NIST is under the jurisdiction of the Science Committee and we would urge the Committee to insist that NIST not rely on politically motivated self-reports but work with the Sector Councils develop objective tests of the Framework's effect on actual security. In the private sector the market generally provides a harsh test to the viability of a product or service. Those products that don't meet consumer demand vanish. The government operates without traditional market forces but it can still use private sector based methodologies for beta testing and cost effectiveness evaluation.

All government cyber security programs ought to be routinely evaluated for their cost effectiveness against specific, previously determined objectives. If a program is not meeting these objectives it ought to be terminated or reformed with its funding going to programs that can be more productive

7. Government Needs to Value People as much as Technology

Well run private sector operations understand the need for, and value of, highly skilled cyber security personnel. Multiple government sources have repeatedly noted the difficulty for the public sector to compete with the private sector for this scares resources which is prima facie evidence that industry places a higher value on these people.

We have already discussed the need for government to dramatically increase its funding of cyber security, but it's equally important that the money that is spent is spent wisely.

One area where the government may be spending its limited funds in a less than optimal fashion is their tendency to focus more on buying technical solutions than on people to operate that technology.

A review just this week in the Washington Post made this exact point when it reported: "After personal information for more than 22 million federal employees and others was stolen, the need for modern technology received far more scrutiny during a series of congressional hearings than the need for skilled people to work it. Search for "cyber" on the Government Accountability Office Web site and you'll find dozens of related documents just this year. But if you ask for a study specifically on cyber talent, GAO will provide one -- from 2011.

Alan Paller of the SANS Institute recently made this very point "Government agencies spend a lot on security but just not correctly. Many agencies are literally bristling with sophisticated tools for detecting and monitoring intrusions and threats but they are mainly watched by personnel who do not know what to do with the data generated by these systems. The tools can find the problem but it's the people who know where to look and what is missing."

In addition to being substantively dysfunctional, government's refusal to spend adequately to attract top quality cyber personnel may actually be costing the government money. An April report from the Partnership for Public Service found that: "As the compensation gap continues to widen, especially for the most talented professionals, the federal government will continue to fall behind, but ironically, private companies not limited by federal pay scales can simply hire away the best cyber security talent and rent it back to the government at a higher hourly rate"[15]

The Report concludes that government needs a master cyber workforce strategy to attract and retain top talent, as without a master strategy in place agencies are operating largely on their own in a haphazard system.

8. Government needs to adopt a more segmented approach to cyber promotion Government's generic education programs lack need to

One of our major problems in cyber security is that we simply do not have enough educated cyber security professionals. Despite developing a better cyber workforce being a consensus goal for nearly a decade we do not seems to be making appreciable progress. This lack of progress is more ironic as cyber security jobs are high prestige and high pay, yet the market has not been properly stimulated.

One problem is that the federal government's approach to the cyber workforce development is generic. For example research demonstrates that school guidance

[15] http://ourpublicservice.org/publications/download.php?id=504

counsels has generally very little awareness of cyber security career paths and hence are not channeling promising students into this career option.

A market segment approach needs to be adopted by the federal government so they can more effectively use the funds to be devoted to cyber security workforce promotion. In the private sector target segments are carefully drawn and specific marketing campaigns based on consumer research are designed. The federal government needs to adopt these private sector practices to its cyber workforce development programs.

9. Government needs to leverage the private sector more creatively to create a more effective cyber workforce development. Contemporary institutions such as gaming and ESPN can be leveraged to more effectively reach the millennial target audience

One of the most critical steps we, all of us public and private, who are being subjected to the constant cyber assaults need to do is leverage our resources far more efficiently to create sustainably secure cyber eco-system.

The attack community not only has "first mover" advantage forcing us largely into a responsive mode to novel attack methods, but they are better organized than we are. They are more flexible than we are. They are being more innovative than we are. They have a more efficient and effective financing system than we do.

All the economic advantages in the cyber security eco-system favor the attack community. Attacks are comparatively cheap and easy to access. The attacker worldwide business model is highly efficient. Cyber-attacks are tremendously profitable. On the defense side we are almost inherently a generation behind the attackers. It is difficult to demonstrate ROI to preventing attacks. Consumers, including the federal government, are not putting an appropriate economic value on cyber security ---preferring functionality and low cost-- to security. The interconnected nature of the system exacerbates the vulnerability even of good actors, which could undermine investment. And, there is virtually no law enforcement. We successfully prosecute maybe 1 or 2 percent of cyber criminals.

It is absolutely critical not only for the federal government to learn from the private sector but that it also contributes more effectively to the collective defense effort. One place to start is with more creative education and outreach programs

For nearly a decade DHS has been running an outreach program called NICE which is outdated and lacks needed imagination to reach the generation that will drive effective workforce development.

NICE's slogan, Stop, Think, Connect, is straight out of the dial up age ---millennials, in fact almost no one stops and thinks before they connect to the Internet---we have long been in an age where people are virtually always connected. Millennials often sleep with their smart phones on, connected and receiving.

Instead of NICE, the four letters DHS ought to focus on is ESPN. As is being pioneered in Asian countries the Gaming world is being targeted with tens of thousands of your, tech-savvy players attending tournaments and hundreds of thousand "tuning in" on line.

DHS ought to collaborate with private entities like DHS and find a way to market these programs and blend cyber security elements into the spectacle. Promotions and camps could be provided in partnerships that would capture the joy millennials get from gaming and steer at least a portion into cyber security education and carriers.

10. The federal government needs to treat the private sector like true partners, not stakeholders

Government need to appreciate that with the private sector owning and operating the vast majority of cyber infrastructure, and being subjected to attacks form nation states on private enterprise, the traditional roles for government and industry many not apply in the cyber security context.

Improvements can be made in many areas including tactical, such as more effectively sharing information. However some of the work that needs to be done at a broad conceptual level such as working through a coherent policy for the role of the federal government with respect to assisting the private sector when it is attacked by nation-state or state affiliated attackers.

A useful place to start would be for government to stop blaming the corporate victims of cyber-attacks. The annual report of the Pentagon for 2015 states that most DOD systems are subject to being compromised by low to middling level cyber-attacks. In such an environment it's reasonable to ask what level of security we ought to expect from discount retailers and movie studios. Some cyber experts have claimed that as much as 90 percent of the cyber-attacks they are working on have at least some element of nation state affiliation. James Clapper stated just last month that it is unfair to be blaming these victims in the press when they are fighting off irresistible foes.

At a more operational level government needs to work with industry to create an organizationally coherent cyber eco system wherein trust can be established and we in the defenses community can better leverage our resources in the face of the better organized attack community.

ONE PAGE SUMMARY OF TESTIMONY OF INTERNET SECURITY ALLIANCE PRESIDENT LARRY CLINTON ON WHAT GOVERNMENT CAN LEARN FROM THE PRIVATE SECTOR ON CYBER SECURITY

1. Federal government must invest much more in cyber security. The private sector is investing at a far greater rate with increase rates two and a half times as much as federal non-defense spending. Just two banks spend 25% more than all of DHS
2. Government must act with greater urgency. It took 6years to pass a modest info-sharing bill. Four years after the House GOP Task Force Report on cyber security there has been almost no progress on its top recommendations
3. Top policy makers need to be educated about cyber security. The private sector is educating its top management, such as corporate boards with dramatic policy impact. We need an education program for government equivalents to corporate boards including Members of Congress
4. Government needs to reorganize for the digital age. The private sector is moving to an enterprise wide approach to cyber security. Government is still fighting turf wars which inhibits progress and wastes scarce resources
5. Government needs to adopt a risk management approach to cyber security. Government ranks last in adopting standards and fixing problems because it uses check list security instead of risk management as the private sector does
6. Government needs to assess its own programs for cost effectiveness. Unlike the private sector programs like the NIST Framework were not beta tested so we have no objective data as to their actual effect on improving security.
7. Government needs to focus more on people as opposed technology. Government tends to be over reliant on tech solutions to cyber problems while the underinvestment in people undermines the effectiveness of tech
8. Government needs to adopt a more segmented approach to cyber promotion Government's generic education programs lack need to be segmented and targeted similar to the process the private sector uses
9. Government needs to leverage the private sector more creatively to create a more effective cyber workforce development. Contemporary institutions such as gaming and ESPN can be leveraged to more effectively reach the millennial target audience
10. Government needs to treat the private sector as true partners and not as government stakeholders. The blame the victim orientation of many government agents needs to be reoriented to create a more effective partnership

BIOGRAPHY

LARRY CLINTON
PRESIDENT, INTERNET SECURITY ALLIANCE

2500 Wilson Blvd., Suite 245
Arlington, VA 22201
lclinton@isalliance.org
703-907-7028

Larry Clinton is President and CEO of the Internet Security Alliance (ISA), a multi-sector trade association focused on cyber thought leadership, policy advocacy and promoting sound security practices for corporations. In 2015 Mr. Clinton was named as one of the 100 most influential individuals in the field of corporate governance by the National Association of Corporate Directors (NACD). He is widely published on cyber security and was the principle author of the Cyber Risk Handbook for Corporate Boards published by NACD in 2014 and endorsed by DHS in 2015. He has been featured by WSJ, USA Today Fox News, NBC, CBS, NYT, PBS Morning Edition CNN & MTV. He testifies often before Congress; He has briefed industry and governments world-wide including NATO and the OAS. Mr. Clinton was the principle author of the ISA Cyber Social Contract which outlined a market based, as opposed to government regulatory model, for improving cyber security. The document's recommendations were adopted by the House GOP Task Force on Cyber Security in 2012 and it is also the first and most often cited, reference in President Obama's principal policy paper on cyber security. In 2013 the President's Executive Order on cyber security adopted the ISA's market incentive "social contract" model to promote national cyber security.

Chairwoman COMSTOCK. I thank the witnesses for their testimony, and we now will move to questioning. I will recognize myself for the first five minutes.

Thank you all so much for your expertise and your passion about this important issue. I remember back in 2014, I was able to sit down with Mr. Wood, and we spent a pretty long afternoon identifying a lot of the problems, and I'm sorry to say that everything you said came true and all the problems you identified were dead-on, but I appreciate that you're here to help us address that.

I was at the consumer technology conference earlier this week, and so we're seeing a lot of the new things that are in practice, and certainly the concept of "innovate or die" is very much a reality here.

So I was wondering, because I think you've all addressed a little bit, but how do existing government contracting provisions impact the ability for the public sector to be agile and to be able to do what you do in the private sector? I know this is a little bit out of our jurisdiction in terms of government contracting but sort of identifying the problem and how we can address it. You know, we have the standards, we have the practices. We know we need to be more risk management-based instead of just a checklist. How can we all get those type of policies in the government that are as agile as what you're dealing with in the private sector? Do you want to start, John?

Mr. WOOD. One suggestion I would have is that I think it would be very helpful for the government to move more towards a best-value approach to government contracting versus lowest price, technically acceptable approach. The same individuals that we put on assignment with the government often we will receive a much higher rate for those individuals when we're working commercially because commercial companies tend to value the kind of capabilities that our security professionals have, and when I say "much higher," often it's, you know, 200 to 300 percent higher, and I think at the end of the day, that's a really big issue that the government needs to at least address, because otherwise you tend to get what you pay for.

Chairwoman COMSTOCK. Yes, Mr. Clinton?

Mr. CLINTON. I agree completely with Mr. Wood, and I think this speaks to part of the education issue that I was speaking to. We need to have a better understanding of the breadth of cybersecurity. What you're talking about, Madam Chairman, is frankly not an IT problem; it is an economic problem. That's what cybersecurity is. It is not an IT problem, it is an economic problem, and we need to find a way to move away from, as Mr. Wood said, lowest cost items, particularly in the federal space. We have examples where federal agencies are buying equipment off eBay from non-secure suppliers because it's lower in cost, and while we appreciate the tension and the need for economy in these times, we have to understand that there is a direct tradeoff between economy and security, and we're just going to have to come to grips with that, and we haven't. I think if we could educate the federal leadership in the way we're educating corporate boards—where by the way we had exactly the same problem a few years ago. We might be able to get a better appreciation of the interplay between the economics of cybersecurity and the technology of cybersecurity.

The real problem that you're speaking to, in my opinion, mostly comes in the smaller business elements of cybersecurity. If you're going to deal with, for example, the major defense contractors, frankly, you compensate them perfectly well and they have pretty good cybersecurity, but because of the procurement system, they are required essentially to farm out a lot of the procurement to smaller firms across the country in Congressional districts and those smaller firms do not have the economies of scale to meet the cybersecurity standards that the primes have. We have to find a way to provide incentives for those smaller companies to come up to grade because it is not economic from their business point of view in order to do that. Now, we think that there are a number of suggestions that we've made and I referred to in my oral statement and in the trade association paper that can talk about how we can better incentivize the smaller companies so that we can get them up closer to where the majors are, and if we can do that, we can achieve our goal, which is a cybersecure system as opposed to cybersecure entities.

Chairwoman COMSTOCK. Mr. Schneider?

Mr. SCHNEIDER. I think another thing—this isn't directly a contract issue—is to use the tools that they've already purchased. I think one thing we see a lot in both the private sector and in the public sector is the acquisition of technologies that then aren't even configured properly and used properly. So a lot of the investment that happens both within private organizations as well as the public organizations is to take the technology purchases and make sure that you have the right human capital and the right best practices to deploy those properly. I mean, the most cost-effective thing you can do is use the money that you've already spent more wisely, so I think that's one key that we see as well.

Chairwoman COMSTOCK. Okay. Thank you.

Dr. Casado?

Dr. CASADO. Just kind of quickly more on a positive note, I'm kind of a personal success story of this, so when I graduated with my Ph.D., I was thinking about being a professor, and instead I started working in the intelligence community, who decided to fund a startup that we were doing, and they were great to work with early on, and kind of to Congressman Beyer's point, I do think that there's a lot that we can learn from the government, and that turned into kind of one of the largest tech acquisitions in the private sector ever and a huge security initiative. So I think, you know, more working with the startup ecosystem—I mean, I'm a Silicon Valley guy—but more working with the startup ecosystem, funding that, allowing us access to the way that you think about the security technology I think will hugely help innovation.

Chairwoman COMSTOCK. Thank you, and I want to particularly note the—I think, Mr. Wood, you call it the fifth war fighting command is cyber here. I'm running out of my time, but if we can get—and Mr. Clinton, the numbers and the comparison between private sector and the public sector and what we're spending and sort of the quality, I think that's a very helpful contrast and understanding. This is part of our defense system, and certainly as we've seen social media being used in the terrorism area and all those. So I appreciate you putting real emphasis on that. Thank you.

And I'll now recognize Mr. Lipinski.

Mr. LIPINSKI. Thank you. There are so many things to talk about here, and I just got set off in another direction by what Dr. Casado had just said, so first I'll say it's good to see a Stanford and Berkeley guy be able to sit next to each other. I'm a Stanford guy.

So I'm going to ask Dr. Casado, you had just mentioned there should be more done by the government to engage Silicon Valley entrepreneurs. What more could the federal government be doing right now in this area?

Dr. CASADO. I'm actually very positive about the actions that the government has taken over the last few years. I mean, I've worked with Incutel, I've worked directly with government agencies, and I think continuing to fund efforts that engage directly with startups, understanding that they're risky propositions and understanding that there's a high level of risk, I think is very beneficial. Again, I mean, all of the work that I've done in the last eight years has been based on my experience personally in the government and then funding from the government and it's turned into a major industry initiative, and so I would just encourage you to continue a lot of the work that you're doing, and——

Mr. LIPINSKI. Is there anything that's not being done now that you think should be done on the federal government side of engagement?

Dr. CASADO. Well, I think—I mean I think—I think it—the problem is, you're great at funding on the early stage, and then I think when things get a little bit bigger, it's harder for the startups to engage with the government because you get into these difficult procurement processes that are kind of owned by a number of people. So I would say normally what happens is, you do a great job kind of getting these guys incubating and then they find out that we can't really actually sell to the government because it's too hard and it's too sticky, so we go ahead and sell it to the private sector.

So one thing that you could really help out with is not only get these guys incubated and starting and providing them the initial funding but actually give them inroads into selling to the government, being an actual vendor to the government and helping that out. That was my—so originally we tried to actually engage the government, and it wasn't until eight years later that we could actually do it in a viable way, and now we're doing it in a way that we're very excited about, but actually having hand-holding of the procurement process early on would have been hugely helpful.

Mr. LIPINSKI. Thank you.

Anyone else on this subject before we move on? Mr. Schneider?

Mr. SCHNEIDER. Yeah, we're starting to see a lot more engagement in Silicon Valley from various elements of the government. One example is the DHS has obviously been very active over the last couple of years. There's a new DOD project called DIUX where they've now established in Moffett Field right across from Silicon Valley trying in much the way that Incutel's been able to invest in startups to bring some of their technology needs to the Valley, so I think we're seeing a lot more engagement over the last year.

Mr. LIPINSKI. Anyone else? Mr. Wood?

Mr. WOOD. Thank you, sir. I'm honored to sit on the Commonwealth of Virginia's Cybersecurity Commission as well, and one of the things that I've been encouraging the Commonwealth of Virginia to do is to encourage much closer relationships between the university ecosystem and the business ecosystem, and to really promote research. I think that will help propel a lot of the startup activity that the gentlemen to my left are both talking about. Whether it's in Silicon Valley or Research Triangle or in the State of Virginia, at the end of the day we need far more research than we currently have, and the reason is because when I talked about earlier the dollars, the difference between spent in the federal government and the commercial side, it's very simple. We have a real scarcity of resources in terms of cybersecurity professionals, and so we need more tools being able to deal with the complex environment that's going on out there and those tools, i.e. automation, are the way forward, I think, in order to help deal with that scarcity of personnel resources. There are other things we can do as well, but I think that research would really help us a lot from a cybersecurity perspective, really as a nation.

Mr. LIPINSKI. And very quickly, and continuing with Mr. Wood, I want to thank you for your work in STEM education and thank you for bringing up how important it is that the human behavior is critical in preventing so much of this, and I think you said nearly all of these attacks could have been avoided with better behavior, and I think that brings up the importance, as I always talk about here, in understanding human behavior and funding social science research into things like this.

But the last thing I wanted to ask you is, you talked about insurance, and I'm very interested in how do we incentivize the private sector. Is this something that you think should be required or do you just think that this will develop over time? Do you see a need for the government to require insurance for these—against these types of attacks?

Mr. WOOD. Sir, I personally don't think there's a need for the government to require it because I think the lawyers will—at the end of the day will help corporations and other organizations understand the legal liability associated with not taking the appropriate actions.

Mr. LIPINSKI. Have companies really suffered that much who have been—who've had these data breaches?

Mr. WOOD. Oh, I definitely think they're beginning to. I'm seeing more and more boardroom kind of calls being made to our company than ever before. I think the very public retail breaches that have occurred are now heading into not just the CEO's office but right into the boardrooms. So I also believe that the critical infrastructure industries that we have out there that are already regulated feel the pressure associated with doing something, and that's why I think that the insurance companies are doing what they are in terms of really trying to promote cyber insurance. Their feeling is that if they can—if the corporations can provide evidence that they are doing what's appropriate from a risk management point of view, that that will result in two things. One is lower premiums to the corporation who is looking to get the insurance, and then secondly, a better legal defense to the extent that they are sued.

Mr. LIPINSKI. Thank you. I yield back.

Chairwoman COMSTOCK. Mr. Clinton wanted to——

Mr. CLINTON. If I could just very quickly, Mr. Lipinski, first of all, we're big fans of insurance so we've been promoting cyber insurance for over a decade, but I don't think that a requirement is appropriate, and——

Mr. LIPINSKI. If you've been promoting it for over a decade and it doesn't seem like it's that widespread, is it?

Mr. CLINTON. No, and that's because of systemic problems within the insurance market, the lack of actuarial data, and in particular, the enormous risk that the insurance companies realize that if they insure and there is a major catastrophe, they're on the line for everything.

We faced the same problem in terms of insurance in the last century with crop insurance and flood insurance, and there are systemic ways that we can work with the federal government in order to address that problem, and I'd be happy to go into those in some detail, but I wanted to get to the specifics of the requirement piece.

I think one of the things the federal government could do is require insurance, cyber insurance, for your information systems in the same way that you require physical insurance when you build buildings and everything else, and I think if the government did that, it would be a market leader in that regard.

The other thing I just want to point out, and this bears, I think, a little more conversation because I think this is a widespread misnomer, of the reality when you look at the data of the economic impacts of the high-profile breaches is not what you think. If you go back and look 6 months after the Sony attack, their stock price was up 30 percent. If you go back and look at six months after Target, the stock price was up about 26 percent. If you look at most of the high-profile breaches, you find that there's an initial reduction and then there's a bounce back, and I can explain why that is, because the smart guys on Wall Street say ooh, nice distribution system, I like the price point of their products, and ooh, the price is down, buy opportunity. So the natural things that we assume are going to happen really are not happening when we look at the data, but Mr. Wood is exactly right about the fact that corporate boards are spending much more attention on this, but I think that has to do more with the threat to their intellectual property which is being vacuumed out and is a tremendous economic risk.

Mr. LIPINSKI. So they're not concerned about the consumers and the people who are using their business, they're——

Mr. CLINTON. Well, no, they're——

Mr. LIPINSKI. —concerned about their own——

Mr. CLINTON. Yeah, so——

Mr. LIPINSKI. That's a suggestion there, that——

Chairwoman COMSTOCK. We're going to have to move on to our next question.

Mr. CLINTON. I will get back to that but——

Chairwoman COMSTOCK. And please do submit——

Mr. LIPINSKI. Okay.

Chairwoman COMSTOCK. And I'd appreciate you submitting some more information on the insurance area. I think that would be very interesting.

Mr. CLINTON. Sure.

Chairwoman COMSTOCK. And I now recognize Mr. Loudermilk for his five minutes.

Mr. LOUDERMILK. Thank you, Madam Chair.

And after spending 30 years in the IT industry myself, I can equate to a lot of what you're saying, especially the cyber insurance. Big supporter of cyber insurance simply because of the standards that the insurance companies put upon these businesses, and I sold my business a year ago, was greatly relieved when I sold the business because while cybersecurity was on my mind 24 hours a day owning this small company and managing it, it was not on the minds of my customers.

Mr. Clinton mentioned eBay. We had many instances where we put a secure network into place, a network of a small government managing power distribution systems, and we engineer it, we put the products in, some of the products that some of you represent everything from spam filters, firewalls, gateways, content managers, bandwidth managers, and then we would find out that they would go and buy parts for these off of eBay that would come from somewhere overseas, and we don't know the firmware that's on it, and I understand that what's on their mind, especially when you're dealing with small businesses, is bottom line. Doctors are being doctors, lawyers are being lawyers, they are doing what they're doing. We're supposed to take care of that. But when we go forward and we say this is what we need to do to upgrade and say we don't want to do that right now, do we have to do it? Well, your network will still function but you're at a high amount of risk. Well, that usually doesn't change their mindset. So having those sets of standards I think is important.

Another thing that was brought up is this risk-based management. That's what we live by. We used to emphasize to our employees, there's two types of computer users: those that have been hacked and those that don't know that they've been hacked. Another part of risk management is, we emphasize to our customers, don't keep what you don't need. If you don't need the data, you don't have it, you don't have to secure it.

And that really brings an issue that I have great concern about here in federal government here and that's with the Midas system, which according to news reports is storing information on Americans who access the HealthCare.gov website, not just those who got their health insurance, but those who even shopped it, and it's storing personal identifiable information of Americans without their knowledge in a data warehouse.

And for Mr. Wood, considering what's happened to the federal government, the recent expansive data breaches, does it concern you that the federal government will be holding information on citizens without their knowledge, even for citizens who did not get their healthcare coverage through this system? Am I justified in my concern over the risk of storing this data, especially data that is not needed.

Mr. WOOD. So you're raising both a privacy perspective as well as a cybersecurity, you know, issue. You know, at the risk of being a Monday morning quarterback, you know, which is what I would be doing if I were to reflect on the OPM situation, the very unfortunate OPM situation because like all of you, I also received my letter that gave me the good news. I think that in retrospect, had OPM been using, you know, two-factor authentication, had they been using encryption at rest, had they had log files, we would've had a much different situation than perhaps we ended up having with OPM.

So as it relates to the HealthCare.gov situation, I don't know how they're storing the data to be able to reflect to you about what is appropriate, but I think generally speaking, most people are a little nervous because those of us that are in the know worry that there just isn't enough resources being applied from a financial perspective to the IT security issue, and it's not just at the federal level, it's at the state level too.

Commercial corporations, on the other hand, I see around the world are taking the appropriate steps. You know, I gave the example early on in my testimony about JP Morgan Chase. You know, when they were hacked, they were spending at that time about $250 million. After the customer PII got out, they went to the board. The board looked at it and determined that they had to increase substantially their spend to do a couple things. One was to actually buttress what they were doing from an IT security perspective, but the other thing was to do was to raise the confidence of their customers. So at the end of the day, I would argue that while their shareholder price has gone up over time, they absolutely—and every corporation cares about their customer data. Thank you, sir.

Mr. LOUDERMILK. And I'd like to ask Mr. Clinton to respond to the same question, but also Mr. Wood, part of mitigating your risk is not keeping data that you don't need. Would you agree that that is a good practice, if you don't need data to not store it?

Mr. WOOD. Yes, sir.

Mr. LOUDERMILK. Okay. Thank you.

Mr. Clinton? Microphone.

Mr. CLINTON. I'll say it again: that's absolutely right, sir. Thank you.

Mr. LOUDERMILK. Okay. Thank you.

Chairwoman COMSTOCK. Thank you.

And now I'll recognize Mr. Beyer.

Mr. BEYER. Thank you, Madam Chairman—Chairwoman.

Dr. Casado, I was fascinated by your testimony, especially the—I'm quoting you a little bit: Once the intruders pass the perimeter security, there's no simple means to stop malicious activity from propagating throughout the data center. This whole notion of unauthorized lateral movement and your call for zero trust micro-segmented network environments, interior rooms with locks, is this recognition built into NIST's cybersecurity framework, moving from just the perimeter security to the internal stuff?

Dr. CASADO. Yes. So we're actually working with NIST now but I don't believe it's currently codified within NIST, so I think that making it part of a standard would be greatly beneficial.

Mr. BEYER. It sounds like an essential part of the cybersecurity framework, it should be?

Dr. CASADO. Yeah, I think this is rapidly becoming a best practice within industry and the private sector, and actually in some areas of management as well. I think putting it as part of a standard would be very beneficial.

Mr. BEYER. Closely related to that, Mr. Schneider, you said, and I quote again, "We are well past the days when a password, even a complex one, will be much more than a speed bump for a sophisticated attacker, and multifactor authentication, combining something you know like a password with something you don't know like a text message is essential for any system to be secure. Is this part of the cybersecurity framework that NIST developed?

Mr. SCHNEIDER. I think it's very similar in that it's a best practice that's not codified directly into the framework but it's something that in the ability to protect your information is becoming an industry best practice. The example I would give in the discussion about in the future there probably should not even be passwords as a core element of how we access information because it's so eminently hackable, and we really feel like a future with rich, multifactor levels of authentication is the right approach, and you can imagine yourself. You go back to your office afterwards, you sit down to check your email. If you're using a mobile device that tracks your location, there's already two or three factors of authentication that say I'm supposed to be in my office, I'm in my office, I'm accessing email, my device says I'm there, you may then ask for a PIN or additional kind of level of authentication but it's really having those kinds of dynamic authentication we see in the future and not static passwords that have been such a broken part of security today.

Mr. BEYER. So both of these are evolutions to CSF, which leads me to Mr. Wood. You wrote very eloquently on page 4 of your testimony that "most businesses would prefer the government impose the fewest possible requirements on them." We hear that every day in the House. But how many breaches will it take before it's recognized that allowing the private sector, especially critical infrastructure companies, to choose the path of least resistance creates an opportunity that might put our citizens' personal information at risk, put our critical infrastructure at risk and put our national economy at risk. NIST standards, the CSF, is purely voluntary. When do businesses come together to recognize that this really needs to be the mandated standard across the country?

Mr. WOOD. So earlier we were talking about insurance, and the insurance industry and why hasn't it adopted more cyber insurance more quickly. The simple reason is because there was no standard, there was no agreed upon standard until not that long ago, and so I think that ultimately I look at the NIST cybersecurity framework as a baseline, and what these gentlemen are talking about are in fact good points, and they are additive to the baseline, if you will, but if we can all get to an agreement about what the baseline is and we all adhere to a baseline, at least we know that the other person I'm dealing with is going to be able to evidence for me that I can do business with them because they're taking the appropriate steps.

Mr. BEYER. It just seems to me—thank you very much—that we look at so many things that affect us and we have mandated it, and the regulations have to be cost-effective, but we did airbags in cars and 5-mile-an-hour bumpers and seatbelts, you know, healthcare in terms of the FDA. This may be, if it really is this huge threat to our national security and to our personal security, that we think about mandatory standards rather than voluntary, rather than relying on the threat of a lawyer's lawsuit and insurance to somehow cover this. Mr. Clinton?

Mr. CLINTON. With respect, sir, I would push back the opposite direction. I would point out that in my testimony I pointed to the fact that the federal government, which basically does operate in the model that you're taking about with FISMA standards that they must comply with, et cetera, and when we evaluate them independently versus the private sector, the federal government comes out dead last. The reason is, is that this is not airbags, this is not consumer product safety where there's some magic standard that we just come up to the standard and we are set. The problem is not that the technology is below standard. The problem is that the technology is under attack. That's a very, very different problem. We need to be forward looking. If we talked about mandating standards a couple of years ago, we'd probably be talking about mandating firewalls and things like that that we now see as basically obsolete, and all of our companies would be spending a lot of money complying with these outdated standards. So we need a different model. The digital age is much more forward looking. That's why the Obama Administration and the House Republican Task Force and the private sector all agree that what we need is a forward-looking, incentive-based model and we need to get industries to understand that it is in their best interest to be continually advancing security. They can't be looking backward; they have to be looking forward.

We can do this, by the way, but it is a completely different mindset, and I think we need to understand that in the digital age, the old model just isn't going to work for this modern problem that includes nation-states attacking private companies. There's no minimum standard that's going to protect them. We need a different model, and we think we can develop that, but it is going to be different.

Chairwoman COMSTOCK. Okay. Now I recognize Chairman Smith.

Chairman SMITH. Thank you, Madam Chair.

Mr. Wood, let me direct a couple of questions to you, but let me describe this scenario first, and then ask you to comment on this particular situation. Let's say a senior government official at an Executive Branch department approached your company to set up a private email account and server for conducting both official and personal business. These emails could include sensitive or classified information about national security. In addition, all emails would be stored on a server located in their private residence. Cyber-attacks and attempted intrusions would be obvious threats, among other security risks. The material being transmitted on the private email account could be a matter of national security.

So two questions. Could this scenario unnecessarily expose classified information to being attacked?

Mr. WOOD. Yes.

Chairman SMITH. Do you want to elaborate, or that's pretty clear?

Second question is this: How would your company respond to such a request?

Mr. WOOD. We wouldn't do it.

Chairman SMITH. Does any other witness want to comment on the scenario? And if——

Mr. WOOD. Well, for the simple reason that you're exposing classified data in the open, and at the end of the day, that's—that would not be prudent and would also be illegal.

Chairman SMITH. And why illegal?

Mr. WOOD. Because the government requirement is that all official information be used through official means, meaning through government networks.

Chairman SMITH. Okay. Thank you, Mr. Wood. I don't have any other questions, and yield back, Madam Chair.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Tonko.

Mr. TONKO. Thank you, Madam Chair.

All of this hearing isn't focused on research. I know that Mr. Wood had addressed research as a component for growth in this region, in this area.

As you know, the government plays an important role in supporting cutting-edge research on all aspects of cybersecurity from prevention to detection to recovery. And through agencies such as the National Science Foundation, the National Institute of Standards and Technology, and the Department of Homeland Security, we fund everything from basic research to testbeds for emerging technologies. And all these federal investments in cybersecurity R&D are coordinated under the longstanding networking and information technology R&D programs.

So while Mr. Wood did raise the issue of research, are there recommendations that you, Mr. Wood, or any of our individuals who are testifying, any recommendations that you would have about federal agencies and how to set research priorities and what major research gaps might exist out there so that we can better partner in a more effective manner with research opportunity? Mr. Wood?

Mr. WOOD. Sir, thank you for your question. I agree. I think the national labs are doing a tremendous amount of work around all kinds of initiatives that regrettably many don't see the light of day ultimately. I think more can be done to, A, make industry aware of what the national labs are up to, and then B, provide a mechanism for industry to license some of those very critical research and development initiatives that really may have one specific customer but ultimately could have an entire industry that it could help serve. I think that would do a couple things. One, it would provide potentially an income stream back to the labs and therefore the government, and the other thing it would do is provide, if you will, more innovation without having to spend a whole lot more dollars. Thank you, sir.

Mr. TONKO. Thank you.

Anyone else? Mr. Schneider.

Mr. SCHNEIDER. One area that we're very invested in right now is on helping kind of the people part of the equation. I mean, technology will continue to be an important element of any security approach and automation underneath, but clearly it's the people on top that we have to make sure are adequately trained, and one of the areas we've been highly invested in over the last couple years is simulation platforms to help us all understand what cyber breaches look like, what cyber incidents look like and be able to respond to those. So many companies today, for example, they send out fake phishing emails to their employees and see whether they respond or not, and if they report it to their security organizations. That's one simple example. There's also simulation platforms that take real-world breaches and model those and allow security professionals to interact with those. So that's an area that's been, I think, on the DOD side, you know, things like cyber range initiatives, very mature for a number of years. This is really now coming into the private sector and civilian agencies and a scenario that Symantec has invested heavily in, and I think there's a lot of potential for cooperation with some of the labs.

Mr. TONKO. Thank you.

Mr. Clinton?

Mr. CLINTON. Mr. Tonko, perhaps a slightly different level of abstraction. I think we would strongly support the notion of the government doing some research on the cost-effectiveness of the NIST framework. We are big fans of the NIST framework. In fact, we like to think it was our idea. At ISA, we published material on this a number of years ago. The Executive Order says it's supposed to be prioritized and cost-effective and voluntary. We believe that if properly tested, we would be able to determine various elements of the framework, and the framework is enormous and applies in different ways to different companies and sectors, but I think if we did cost-effectiveness studies, we could demonstrate what elements of that framework are most effective to varying sizes and sectors of industry, and once you can demonstrate that the framework is cost-effective, you don't need mandates for it. Companies will do what it is cost-effective. But when you go to a boardroom, you know, you can't just say hey, this is a great idea and Congress passed it. They're going to say where are the numbers, you know, show me that it's cost-effective, and if we did that kind of research, which is pretty easy and pretty inexpensive, I think we could get a lot of bang for the buck in terms of doing what I think we all want, which is for industry to adopt these things on a forward-looking voluntary basis.

Mr. TONKO. Thank you, and Dr. Casado, please?

Dr. CASADO. Yes. I think for the last 15 years, I've had a lot of experience getting kind of research grants from the government. I was a research scientist in the National Lab. You guys, you know—DHS paid for my Ph.D. program. I was a DHS fellow and started my company. I've done a number of research grants while I was at the Ph.D., and the biggest difference in my experience between very useful funds and not very useful funds is the number of constraints that are on them, so more flexibility in applying funds to our direct research agenda led to better research. So I think the more agenda that goes prior to the funding, the harder it is for us to basically fit it within our broader research agenda, and so I do think that it's great to fund certain areas. I don't think it's so great to overconstrain the problems that are being looked at.

Mr. TONKO. Thank you very much, and with that, I yield back, Madam Chair.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. LaHood.

Mr. LAHOOD. Thank you, Chairwoman Comstock, and I thank the witnesses for being here today and for your testimony.

Question: When we talk about cybersecurity and these breaches whether in the private sector or in the government, and whether we describe them as hackers or something more sophisticated, every time this is done either in the private sector or to a government agency or entity, would you describe that as criminal behavior? Is that a violation of a state or federal statute in some respect?

Mr. SCHNEIDER. I think one of the challenges of cybersecurity is it's a global phenomenon, and many of the attackers are not in the United States and they're not in a particular state in the United States, but the assets that they're protecting may be. So I think the legal kind of considerations can be pretty complicated.

The other thing is, as more and more infrastructure moves to cloud platforms, which are also deployed globally, even where those assets are becomes more of a challenge. So I think in general, the answer is yes, but there's a lot of complexity to the global nature of cybersecurity.

Mr. LAHOOD. And I guess as a follow-up to that then, you know, if we look at, you know, traditionally when there's criminal behavior that is engaged in, eventually there's somebody held accountable or responsible. There's a prosecution, there's a legal process that happens. I guess the question to you is, are you aware of a successful prosecution where somebody's held accountable, where there's a deterrent effect? It seems like there's no penalty, there's no pain, there's no consequences to anybody that engages in this activity. Yeah, Mr. Clinton?

Mr. CLINTON. Yeah, Congressman, I think you've put your finger on what I would think is one of the number one problems in this space. I would answer that it absolutely should be criminal, in many instances is criminal, but as Mr. Schneider points out, it's not in certain places so we need to be doing two things. We need to be dramatically increasing our law enforcement capability. As I said in my testimony, we are successfully prosecuting maybe one percent of cyber criminals. There's no deterrent really on the criminal side or no viable deterrent. So we need to be dramatically helping our law enforcement guys who are doing a great job but they are underresourced dramatically, and then we also need to be working aggressively with our international community to create an appropriate legal structure in the digital age. We don't have it. We are operating in an analog world with cyber-attacks and it simply is unsustainable. We need to be doing both of those things.

Mr. LAHOOD. And I guess, is there anybody that's leading the way on that, Mr. Clinton, out there either, internationally or here domestically? I mean, where are we at with that process?

Mr. CLINTON. We are not doing nearly enough. I mean, there are people who will give a speech here and there, and again, I'm not going to point fingers at law enforcement. I think they're doing everything they can. They're underresourced. I think we need leadership from the Congress to demonstrate that this is a priority and we are going to fund it much more aggressively.

Mr. LAHOOD. Thank you.

Yeah, Mr. Wood?

Mr. WOOD. Thank you for your question, sir. The issue is that from a law enforcement perspective is first of all, as Mr. Clinton pointed out, it requires, you know, global cooperation but then the standards of prosecution also have to be the same. So in other words, a standard of prosecution here at the federal level might actually be different than at the Commonwealth level, which might actually be different than in Paris. So I think there needs to be some agreement as to what the standards are for prosecution as well.

Mr. LAHOOD. Yeah, but why are we waiting around for that? It would seem that this is ongoing, there should be some standards set to do that instead and it doesn't sound like there's a framework in place to even address that.

Mr. WOOD. We did an analysis in the Commonwealth on just that point. You know, it was a really great analysis which I'd be more than happy to provide to you from the Commonwealth of Virginia. I don't know why. All I can say is that the standards even within the states are different for prosecution.

Mr. LAHOOD. And can you point to me in the Commonwealth of Virginia where there's been a successful prosecution or that deterrence has been put in place in Virginia?

Mr. WOOD. We just changed the laws within the last six months, and I'd have to refer to my colleagues in law enforcement to let you know.

Mr. LAHOOD. Okay. Thank you. I yield back.

Mr. WOOD. Thank you, sir.

Mr. SCHNEIDER. Actually, one point if I can.

Mr. LAHOOD. Go ahead.

Mr. SCHNEIDER. There are a number of great examples where there's been cooperation between the private sector and law enforcement to do takedowns. I could give you a number of them. I mean, Gameover Zeus is a recent one where Zeus has been a financial fraud botnet that's been around, very successful for a number of years. It was put out by a private-public partnership. The next version of that came online. Symantec and a number of private companies as well as FBI and Europol brought down that botnet. And this is the botnet that actually was really propagating things like Cryptolocker, which maybe you heard about, where it takes people's machines and encrypts all the information and extorts you to get that information back. So there's some very kind of successful examples, but I think to your point, a much more consistent global approach is needed.

Mr. LAHOOD. And in your case—I appreciate you mentioning that—was there actual individuals held accountable? They're in prison right now?

Mr. SCHNEIDER. Yeah, there's a particular individual in Eastern Europe that has been prosecuted and convicted.

Mr. LAHOOD. And are they in the United States in prison?

Mr. SCHNEIDER. No. It's in Europe.

Mr. LAHOOD. Thank you.

Chairwoman COMSTOCK. Thank you, and I now recognize Ms. Bonamici.

Ms. BONAMICI. Thank you very much, Madam Chair, and thank you for holding this hearing. It's such an important issue, and certainly one where there's a lot of room for bipartisan cooperation. I think Mr. Clinton identified the challenge of setting policy in this area because the technology always changes so much faster than policy changes, so that being said, I really look forward to working with all my colleagues and continuing to raise awareness about this important issue, and also come up with policy that not only addresses the issue but prevents it.

I was recently out in Oregon visiting ID Experts, which is an Oregon business that specializes in healthcare, health data breaches. This is not just a federal issue, as some of my colleagues might have suggested. I mean, look at the Anthem Blue Cross. We're talking about millions of people here. And most people think—when they think about identity theft, think about the financial consequences, but with medical identity, if someone gets a procedure or prescription or something and that is entered into the individual's electronic health records, there are health risks involved in that as well as financial risks, and it's no surprise that the majority of people don't carefully review their explanation of benefits statements just like a lot of people don't carefully review their financial statements, their credit card statements that might alert them to something.

I want to follow up on something Mr. Lipinski started this conversation about the psychological aspects and ask you, Mr. Schneider, in your testimony you say this is—put a picture in my mind here like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals lie in wait on legitimate websites that they previously compromised and used to infect visitors. Most of these attacks rely on social engineering, simply put, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology. So now I'm going to have this lion—this vision of a lion waiting and maybe that'll help stop me from clicking on things that I shouldn't click on.

But Mr. Schneider, could you talk a little bit about whether do we need to fund more behavioral or social science research? Do we need to do a better job educating people about those risks and how to identify them? How do we get in—are we adequately addressing that psychological aspect? Because when we talk about the risk, and I think Mr. Casado, you—Dr. Casado, you brought this issue up as well that we have to do more to prevent that. So Dr. Casado or Mr. Schneider, could you address that, please?

Mr. SCHNEIDER. Yeah. I think ultimately social engineering is always going to be part of the security equation because we as human beings are fallible. So I think systems have to be put in place to enable us to do a better job of helping to secure our own information as well as, you know, our company, our agency's information, and I mean, I think some of the examples I would give you, though, are in the training area that we talked about, helping all of us to think more about security, be more thoughtful about security. But secondarily, it's the kind of security architecture underneath that makes it much, much harder for the attackers to get the information that we care the most about. So all the world's information is not created equal. As you identified, medical health records are much more important to us or financial records are much more important to us than the lunch menu that we're going to look at today. So it's taken a much more, I think, granular approach to information protection, identifying the sensitive information that we care the most about and put more security investment around those kinds of assets than kind of the generic assets that are out there.

Ms. BONAMICI. Dr. Casado, what's your thought on that?

Dr. CASADO. Yeah. So I'm 39 years old, and when I was 37, I got an email from my sister on my birthday and it was like, you know, dear brother, I'm so happy you're my brother, and there's a picture of us when we were kids that's really sweet, and then, you know, it was nice to see you last week. There was a picture of us more recently, and happy birthday, and there's a little link and so forth, and I was like—the first thing I thought, this is so sweet, you know, like my sister has never remembered my birthday before, and I thought you know what? My sister's never remembered my birthday before so I looked at the mail headers. It had come from Russia. Now, listen, I've got a technical background and I've got a sister that doesn't remember my birthday, and if either of these weren't——

Ms. BONAMICI. It's now on record.

Dr. CASADO. And if either of these weren't true, I'd have clicked on that link and I would have infected my computer, and I think this tells me fundamentally that it's very important to train users and it's very important to do passwords but a determined attacker will find a way in. I mean, they got these pictures off of Facebook. It wasn't that hard to do. That was probably two hours of work to send me that email, and if I was anybody else, I would have clicked on that link. And so I think that's why I——

Ms. BONAMICI. Can you just both real quickly—I'm almost out of time but I also serve on the Education and Workforce Committee. Where—what are we going to do in terms of educating the next generation and the workforce to make sure that we are getting a step ahead?

Dr. CASADO. Well, I think there's two approaches. I think core education around security perimeters—I think actually Mr. Wood was very, very clear, and I think that these best practices are important. The second thing is, there are technical implements we need to put in place assuming a breach will happen, because it will happen. I mean, it's just a determined adversary will get in. Therefore, we need to implement a zero trust-type model.

Mr. SCHNEIDER. And I think the other point is, there's a huge gap of security professionals in this country today, so creating the educational programs to enable returning veterans and high school and college students to choose careers in cybersecurity is something that's very important as well.

Ms. BONAMICI. Thank you. My time is expired. I yield back. Thank you, Madam Chair.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Palmer, and actually, Dr. Casado, we'll have to work on that birthday if you want to let your sister know right now what the day is.

Mr. PALMER. Thank you, Madam Chairwoman. I'm happy to report for the record that my sister does remember my birthday but my brothers do not.

On that same line, though, Dr. Casado, you can have the best technology in the world, you can have great training, but if employees are negligent in their use of it, you're still exposing yourself, and I bring this up in the context of an article that was in the Wall Street Journal back June—actually it was June 9th, and it relates to the fact that the Immigration and Customs Enforcement Agency had sent a memo to their employees in 2011 because they had seen an uptick in cyber-attacks related to employees using the federal server to access their personal websites or their personal email. Unfortunately, the labor union filed a grievance and prevented them from doing that, and that's apparently where one of the breaches occurred later last year. And my question is, and this would be both for corporations and for the federal government, does it make sense to prevent employees either in the private sector or in the government sector from using their company servers or the federal servers to access personal information—their personal servers, their personal websites, their emails?

Dr. CASADO. Just very quickly, I mean, it seems to me IT goes through these phases where it kind of collapses and expands. We had mainframes, and they went to a whole bunch of computers and then they collapsed recently, and now they're expanding again. You've got mobile, iPhones, clouds, all of this other stuff. I think it's unrealistic from a day-to-day perspective, from an innovation perspective to assume people at work aren't accessing outside information and people outside aren't accessing work information. Every time I travel, I am constantly connected no matter where I go, whether it's vacation or not, and so I think we need to assume that this information is going to be accessed no matter where they are or what capacity that we're running under.

Mr. PALMER. Mr. Clinton?

Mr. CLINTON. Mr. Palmer, I agree with Dr. Casado's comments, particularly with respect to millennials. You know, if you adopt that kind of workforce policy, you're probably not going to be having much of a workforce left to deal with. But I do think that there are things that we can do and we are doing and some in the private sector.

So one of the things we're trying to do is move out of this IT-centric notion of cybersecurity, and for example, involve the human resources departments in this, and what we're advocating and we're seeing some success with is that we are integrating good cybersecurity policy into the employee evaluation system so that, you know, if you have downloaded things you shouldn't be downloading, you know, you are less likely to get that step-up increase or that bonus at the end of the year. We've got to make this part of the overall process. And there are other things that we can do and we are seeing adapted in the private sector such as having separate rooms with separate equipment so that people can, you know, access their personal information or their data without using the corporate system.

And so I think if we are a little bit more inventive about this and use that more incentive model, we're probably going to have more success.

Mr. PALMER. I think that's a great point because you can have a public access, a separate environment where people could do that but they have to use it because, for instance, if you'd been a federal employee, Dr. Casado, and you had opened that email from your sister through the federal mainframe, would that have potentially infected——

Dr. CASADO. So I've worked in a SCIF. I had four computers that would measure like how far apart they were, so I'm very, very comfortable in these like high secure environments. I just think if you want to be competitive from a business perspective against other companies, you have to assume that your employees are going to be fully connected at all times.

Mr. PALMER. But can you not create a separate environment?

Dr. CASADO. I don't think you can do this without having an operational overhead. I really don't. I think you will limit the ability for the business to function.

Mr. PALMER. Mr. Wood, you wanted to comment?

Mr. WOOD. Yes, sir. I would just want to follow up on what Dr. Casado said. So as the use of the internet increases and as the "internet of things" becomes more prolific, everything has an IP address, so where do you draw the line? At some level I would almost prefer that people use my infrastructure because I know what we do from a security perspective. I don't know what they do from a security perspective. And so to the extent that, you know, you make the argument that there should be some separation, I think there are very good arguments on both sides. I'd rather have them in my infrastructure because I know what we do. Thank you, sir.

Mr. SCHNEIDER. I think the approach that makes a huge amount of sense when you think about all this connectivity is to really understand and protect the information and the identities of the folks that are trying to access it, and that's really what we've seen in security over the last, you know, five-plus years is this move toward not just protecting systems and networks but truly understanding the information and the most sensitive information and putting the right kinds of protection around that.

Mr. PALMER. My time's expired but I do want to thank the witnesses for the clarity of your answers. This has been an excellent hearing.

Thank you, Madam Chairwoman, and I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Swalwell.

Mr. SWALWELL. Thank you, Madam Chairwoman, and I want to first thank each of the panelists for their service and for talking about this important issue, and Mr. Casado, I want to highlight that you graduated from Stanford University in the Bay Area and also that you began your career at Lawrence Livermore National Laboratory, which is in my Congressional district, and so I'm honored to represent the folks there as well as Sandia National Laboratory, and many of them are working on this issue.

And Mr. Casado, your solution for cybersecurity is to wall off certain segments of one's network in order to prevent cyber intruders who have penetrated outer defenses from gaining access to particularly sensitive information. You argue that such new approaches are already the gold standard for commercial industry and need to become the gold standard across the federal government. How much time and resources would it take for the federal government to do this, and are the costs worth the benefits?

Dr. CASADO. That's a great question. So the technology and adoption has evolved enough that we know how to do this without disruption basically so early on it was kind of like well, you know, it's an extremely secure environment and extremely sensitive environment and, you know, we can kind of go and retrofit things and now we've got mostly software-based solutions that you can put in, you can do non-disruptively. Cost-benefits from a business perspective makes sense, so much so that, you know, this adoption is one of the fastest growing sectors of the enterprise software space. So I think it's not only practical but we have enough experience over the last couple of years to see adoption. So yeah, I think that actually this stuff is absolutely worth retrofitting.

Mr. SWALWELL. Great. And just for all of the witnesses, following up on Mr. LaHood's question earlier, as a former prosecutor I too am quite frustrated that it seems that individuals are able to attack networks and individuals with relative little punishment, and I understand the challenges if these attacks are originating in Russia, Ukraine or from state actors, but for non-state actors, I'm just wondering, what could we do internationally to maybe have an accord or an agreement where we could make sure that we bring people to justice?

I remember I asked a high-ranking cybersecurity official at one of our laboratories, naively, I guess, you know, well, are we going after these individuals, and this person kind of laughed, not being rude but just saying we're not going after them, we're just trying to defend against what they're doing, and I agree with Mr. LaHood that until people start, you know, paying a stiff price, I don't know if this is going to change. And I know as a prosecutor, putting together a case like this is very, very difficult, just the chain of evidence and, you know, proving whose fingertips were touching the keys to carry out an attack can be difficult, but what more can we do internationally? Yes, Mr. Wood?

Mr. WOOD. Thank you for your question, sir. So right after—I'll answer your question over a period of time. Right after September 11th, I was sitting in a meeting with a large number of information security professionals from within the intelligence community, and the question was posed in the auditorium where there are about 250 people, when are we going to start sharing information, and the answer came back from one senior person, in 50 years, and the other—another answer came back from another person, not in my lifetime. And it was very, you know, disappointing to say the least.

Now, you roll forward 15 years and you look at where the intelligence community at least in my opinion is today, it's not like that at all. Today I see the intelligence community sharing information in a way like they've never shared it before from DNI on down, and I think what's happened is, as more and more breaches are occurring and as more and more of this culture of trust is occurring, there's a willingness to work together that didn't happen before. I sit, as I mentioned earlier, on the Cybersecurity Commission in the Commonwealth of Virginia, and we work very closely with DHS and FBI and the state police, and they work very closely with Interpol and others, and I can say that there is a spirit of cooperation that I haven't seen in a long time. What is lacking, however, is the resources and the funding associated with actually prosecuting, number one, and then number two, having a common level of standards of what's prosecutorial and what's not.

Mr. SWALWELL. Great. Thank you, Mr. Wood. Thank you all for your service on this issue, and I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Westerman.

Mr. WESTERMAN. Thank you, Madam Chair, and I would also like to commend the panel today for your very informative testimony and also for the zeal that you have in working in cybersecurity, and I believe it's, you know, potentially the war of the future that we're fighting here in cybersecurity, and I'm from Arkansas, and just for personal reasons, Mr. Clinton, do you have any Arkansas ties just out of curiosity? Okay. And I've been listening to the testimony and the answers to the questions. I've got a 20-year-old college student, and I had a fascinating conversation over Christmas, and you guys were talking about how millennials are always connected, and he was telling me that that's a huge consideration where you take a job now, what the connectivity's feed is, you know, and that wasn't something we considered when I was getting out of college but it played a big key in where they would go to work and where they would eventually live. So I know we're in this connected world now.

To follow up on Mr. Swalwell's question, he was talking about being on offense and the prosecution, but from the technology side, is it all defensive or are there proactive ways to combat hackers before they make their attack?

Mr. SCHNEIDER. I mean, I think there's a set of approaches that are not defensive and are much more proactive that are in place today and will continue to expand. So one example is around things like honey pots, so if the bad guys are attacking you and you give them a place that looks like a legitimate part of your infrastructure that they go to and spend all of their time and energy attacking, you protect your real assets and you're able to study what they're doing at the same time. There's also things like shock absorbers where the harder an attacker hits you with traffic, the more you slow them down and do things like tar pitting. So there's a whole set I think of defensive and more proactive defensive measures that aren't offensive, don't go directly after the attackers that are in place today and are actually very successful within the enterprise.

Mr. CLINTON. Congressman, if I may, I think that's of course true, and there are some others, and I think I want to build off this point into having a better understanding of the multifaceted nature of the cyber problem. So for example, you know, one of the technological mechanisms that we use in the private sector is we understand that the bad guys are going to probably get in, you know, a determined attacker will peruse your system, but actually we have more control over the bad guys when they're inside the network than when they're outside the network, and if you are dealing with a cyber crime situation, you're basically dealing with theft, which means they have to get in the network, they have to find the data and they have to get back out. So if we block the outbound traffic rather than trying to block the inbound traffic, we can actually solve the cyber breach problem. They get to have a good look at our data but they don't get to use it at all, and from a criminal perspective, that's a problem. But if you're looking at this from a national security perspective, the attacker may be interested in disruption or destruction. They don't have to get back outside their network. They don't care about getting outside your network. So we need to understand that we're dealing with multiple different cyber problems, some of which are national security, defense critical infrastructure, making sure the grid doesn't go down, et cetera, and we need a different strategy with regard to that than we may need for the strictly criminal or theft problem, and when we have a more sophisticated policy in this regard, I think we're going to be able to make more progress.

Mr. WESTERMAN. And also just to briefly follow up on a question that Ms. Bonamici was talking about as far as developing new workers for the cybersecurity workforce. Are your companies seeing a workforce shortage? Do you foresee a lot of growth for the future in that? Mr. Wood?

Mr. WOOD. We do see an enormous shortfall of cybersecurity professionals. In the State of Virginia alone, the state government has announced that we've got about 17,000 unfilled cybersecurity professional positions just in the Commonwealth of Virginia.

Sir, if I might go back to your other question if you don't mind about offensive?

Mr. WESTERMAN. All right.

Mr. WOOD. It's a question that's very much near and dear to my heart. You know, if someone were to come in my house uninvited and either hurt my children or my wife or take my stuff, I have the right to defend myself, but if someone were to come into my corporate house and virtually take my stuff, whether it be intellectual property or customer data or whatever it might be or financial information, whatever it might be, we need the ability to defend ourselves, particularly if our cyber command is not going to fund itself in a way that gives us the comfort the same way that we have the comfort, I think, as a nation from a standpoint of air, land, sea and space. Thank you, sir.

Mr. WESTERMAN. And Madam Chair, I'm out of time but I would like to plug our Congressional app challenge and encourage all Members to promote that in their district because it does help develop a new workforce for cybersecurity and a lot of other areas.

Chairwoman COMSTOCK. Thank you, Mr. Westerman, and I will also join you in plugging that. I know it's on our website and our Facebook page, and I think the date is January 15th when things are due, right?

Mr. WESTERMAN. Unless you extend it.

Chairwoman COMSTOCK. Now I recognize Mr. Abraham.

Mr. ABRAHAM. Thank you, Madam Chairman, for having this great hearing, and I want to thank the witnesses for giving direct answers to direct questions. That's refreshing and somewhat of a novel idea in a Committee hearing, so kudos to you guys for answering straight up. We appreciate that.

Some of you have espoused the value of sharing cybersecurity information whether it be a cyber threat tread or a cyber crime with certainly other companies or government officials. This last cybersecurity bill that we passed last month, did that help or hurt in this area?

Mr. CLINTON. Sir, I think that that was a good bill. We endorsed the bill. We support the bill completely. The most important thing, however, is that that is not the cybersecurity bill. That's a very useful tool to have in the toolbox. It can help, but it is nowhere near sufficient.

Mr. ABRAHAM. So we need to do more is what you're saying?

Mr. CLINTON. Absolutely we need to do a great deal more.

Mr. ABRAHAM. And just give me your top three recommendations. What would be your bullet points for the new legislation?

Mr. CLINTON. For new legislation, we would like to see the incentive program that has been endorsed both by the President and by the House Republican Task Force put in place. That would include things like stimulating the cyber insurance market that we've talked about earlier today. It would include with providing some benefits for smaller businesses who don't have the economies of scale in order to get in here. It would include streamlining regulations so that we had an opportunity to reward entities that were doing a good job with cybersecurity in the way we do in other sectors of the economy. A lot of the incentives we talk about and I refer to in my testimony are things that we are already doing in aviation, ground transport, agriculture, even environment. We simply haven't applied these incentive programs to the cybersecurity issue and so I think if we did that, we could do more.

And then the third thing would be, I think we need to have a much better, a more creative and innovative workforce development program. We've talked here about the fact that we are we're always connected now and we all know this, but the slogan that DHS uses for their workforce education program is Stop, Think, Connect, which is directly out of the dial-up age. No millennial stops and thinks before they connect. It just makes no sense. We need to be leveraging ESPN and reaching to the millions of young people who are interested in gaming and popularize that and use that as a bridge to get them interested in cybersecurity. We need to be much more aggressive, much more inventive in this space, and by the way, they are doing these things in other countries. We need to be taking a page from that.

And then the final thing that I'll mention is, we would like to see—I'm not kidding. We need an education program for senior government officials like we're doing for corporate boards who are just like you guys: really busy, lots of things that they have to do, demands on their time. We found when we actually educated them about cybersecurity, we got better policy, we got more investment, we got better risk management. We need to be doing that on the government side just like we're doing that on the private-sector side.

Mr. ABRAHAM. Very enlightening. Any you guys want to comment anything else?

Mr. SCHNEIDER. If you think about, you know, threat information, vulnerability information, I mean, for many, many years in the cybersecurity industry we've been sharing those kinds of information, and some of the keys are being able to take it and aggregate it and anonymize it and share it in a safe way because we're taking information that is, you know, specific to a particular industry or a set of customers and trying to gain the security knowledge but not, you know, not put any of that information at risk. So it's something that's been happening for many, many years in the security industry and I think it's an important element but not, of course, the final answer.

Mr. ABRAHAM. Thank you, Madam Chairman. I yield back.

Chairwoman COMSTOCK. Okay. And I will now recognize Mr. Hultgren for his fiv minutes.

Mr. HULTGREN. Thank you so much, Chairwoman. Thank you all for being here. I know a lot of things have already been asked and answered, but as we say around here, not everyone has asked that same question yet, so my turn.

Now, I'm going to try and focus on a couple different things, but thank you. I do think this is so important and I do think the American people, our constituents, are waking up and feeling some of that fear, and wanting to know the right thing to do. So we always want to hear from you of how we can be informing our own constituents of wise decisions along with ourselves, our families and our staff to protect important information. So much of our society, so much of our financial systems is based on consumer confidence, and if there's a feeling that this isn't safe or whatever it is, I think we're going to lose the benefits that much of this technology has, so we want to do this well.

I do want to talk briefly or ask you your thoughts. We've talked a little bit about what government can do better, learning from the private sector, and certainly the private sector is ahead of us in so many areas. We've also heard—I really appreciate it, Mr. Clinton, your response that, you know, for us to say that this is like an airbag problem, it isn't. It's completely different and, you know, so for us to be prescriptive of saying you have to do this, we always pick the wrong technologies always too late. So instead it's really this framework, I think, of a way of thinking of how to solve this problem, but a question I would have is really with impediments that government is putting up to your business or other businesses from new innovation. What would you say may be the greatest impediment that you feel from government from your business innovating or doing what you already do best? Is there something that has been a hurdle that you've had to overcome, Dr. Casado?

Dr. CASADO. So this is going to be an indirect answer to your question, but actually working with the government on the procurement side, something that's very difficult is when there isn't flexibility in budgeting, which I think it's actually difficult for the agencies and the departments to adopt new technology because the working capital that they have doesn't allow them to move as quickly as possible, and so from a purely financial side, more flexibility in their budgeting I think will help them and certainly help us be able to introduce new technologies into the government.

Mr. HULTGREN. Mr. Clinton?

Mr. CLINTON. I would offer two things, Congressman. First of all, we need to really rid our government partners from the "blame the victim" attitude that they have, particularly at some of the independent agencies. I'm thinking of the FTC and the SEC, for example. As we have articulated here, and I think is fairly common knowledge up in Congress, it's been said the determined attacker is going to get in. The fact that you are subject to a breach is not evidence of malfeasance or nonfeasance. Now, there may be instances where you are malfeasant or nonfeasant, and we should investigate those, but breach per se is not one of them, and so we need to move beyond that particular notion.

The second thing that I would say is that the government really needs to get its act together with respect to cybersecurity. Cybersecurity—you're right, sir. Cybersecurity's real hot now so every entity in the government, every state, every locality, they're coming up with their own cybersecurity programs, and a lot of times these things differ just a little bit and so when you try to do these things, you're forced to meet with multiple different compliance regimes trying to do essentially the same thing. Now, we're in favor of the NIST framework and using that, et cetera, but let's have one and let's make sure we're all working in the same direction, because as we've also pointed out, we do not have adequate resources in this space, and frankly, one of the big problems that my companies tell us is that they're spending all their time on compliance, which means they don't have time to spend on security. I have one company that told me a story about how they were following a legitimate best practice quarterly testing, you know, testing your system every quarter to make sure, you know, you've not been invaded, and they had to go from quarterly pen testing to annual pen testing because all their security were too busy doing compliance. That's a 75 percent reduction in a key cybersecurity best practice due to overregulation coming from different elements. We need to streamline that process, have a good process, but have one process that is cost-effective.

Mr. HULTGREN. Yeah. That's great. Go ahead. I think if you both can speak on this, and then I'll be finished because I think this is very important.

Mr. SCHNEIDER. The one point that I would make and kind of double-click on again is education. I mean, there's a huge and growing gap in the number of cybersecurity professionals available, and Symantec's been doing a lot of work with local universities, but it's not just universities, you know, it's primary education, it's getting the boys and girls that are in high school today and actually really focusing on girls as well to think about careers in cybersecurity and the skill sets that goes with that.

Mr. HULTGREN. Mr. Wood?

Mr. WOOD. Sir, I would just echo a comment but just follow on top of it. So yes, the determined hacker can get in today, there's no question, but as to the Verizon breach report focuses on, you know, 94 percent roughly of those hacks could've been avoided, and then you get the hacker has to focus on the six percent or the eight percent, which is a lot harder to get in then because we have the tools, we have the standards, we have the approach.

The second point I make is the NIST framework is indeed something that I think we can all sort of get behind, and I think it's something that at least it's a baseline.

And then the third thing I would say and the last thing I'd say is that look, compliance and mission are not mutually exclusive. You can make compliance work but it has to be automated and it has to be invisible to the guy that owns the mission so it doesn't inhibit their ability to get their mission done.

Mr. HULTGREN. That's a good point.

Mr. WOOD. Thank you.

Mr. HULTGREN. Thank you, all. I'm over time. Thank you, Chairwoman, and again, thank you all for being here.

Chairwoman COMSTOCK. Thank you, and I thank the witnesses for their very valuable testimony today and the Members for their questions. I've gotten a lot of sort of assignments for today and new issues and areas that we need to explore further. So I would like to invite you all to keep an open dialog with us and don't wait for us to call. Please provide us with any additional information that you think or as you see issues going on. This is going to be, as you all said, an exponentially growing problem. You know, we do have a cyber war that is being waged against us and we—it's a little bit like post 9/11 when they're at war with us but we weren't at war with them. And now we definitely have bad actors on all kinds of fronts from individuals to nation-states who are, you know, waging a cyber war on us, and we need to respond in kind and have that be reflected in our budget but also our responsiveness and how we plan and the 94 percent that we can get covered if we get the right systems into place will then allow us to spend our time on those six percent that we can't prevent because I think we all agree here and we all understand that no matter what we do, this exponentially increasing information world, we are going to have breaches because it's a little bit like I was talking earlier about when somebody before the hearing when I was out in Las Vegas, they said it's like asking never to get sick. You know, in the world that we're going to be dealing with, there will be breaches, but what systems do we have in place to identify them, and if it's only six percent that we have to deal with, then our creative resources and all that we need to do can be very quickly identified there and then move on to solve these bigger problems.

So I thank you for the challenges that you've put before us, and the record will remain open for two weeks for additional comments and any questions from the Members so if there are questions that we didn't get an opportunity or people who aren't here, and I thank the witnesses very much. You're excused here and the hearing is adjourned.

[Whereupon, at 11:05 a.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

Answers to Post-Hearing Questions

Responses by Mr. John B. Wood

REP. COMSTOCK QUESTION - *Do you think that government and private industry should be utilizing offensive tactics as part of their cyber security strategy? In other words, should companies be "bringing the fight to the bad guy" by aiming malware or by launching a denial-of-service attack at the servers of the potential perpetrators?*

JOHN WOOD ANSWER:

To best answer that, we have to first ask: Is the federal government willing and able to take the necessary steps to adequately fund its cyber security responsibilities and thus defend our "virtual" homeland with the same vigor it protects our physical homeland? If not, then the government needs to allow for 2nd Amendment-type protections to apply to the virtual world we live in. The government needs to empower the private sector to defend itself.

The percentage of our overall government expenditures devoted to all cyber security-related activities will reportedly be about $19 billion next year, which is less than 0.5 percent of total outlays. Contrast that with the percentage of private sector budgets devoted to cyber security, and the difference is shocking. Also compare the amount that the U.S. Cyber Command will receive to defend cyberspace – roughly $500 million – with the amounts the Army, Navy/Marines and Air Force will receive – about $150 billion each – for defending the other warfighting domains of land, air and sea. I recognize that within those service budgets is funding for some cyber security activities, but the point remains that defense of the cyberspace domain is woefully underfunded. If that isn't going to change, then we need to be empowered to defend ourselves.

The tactics that the private sector might use to provide for our own cyber defense would depend on the circumstances – what the situation or threat is at the time, and what are our capabilities – all of which are constantly evolving.

REP. LOUDERMILK QUESTION # 1 = *Given the number of recent and expansive data breaches of government systems, does it concern you that MIDAS is permanently storing personal and sensitive information of all Americans looking for health care coverage?*

JOHN WOOD ANSWER:

I am not familiar with the operational details of, nor does Telos do work with, MIDAS. As a general rule, I believe that if an enterprise doesn't *need* to store information, particularly PII, then it shouldn't. Even if you have a strong information security system in place and have taken all appropriate steps to defend yourself and protect your information, the risk is too high. There are so many changes happening so quickly in the cyber domain – new vulnerabilities, new malware etc. – that you're taking an unnecessary risk by storing information you don't need.

REP. LOUDERMILK QUESTION # 2 - *Given the constantly evolving nature of cyber security threats, what steps would your company take to ensure that personally identifiable information is not compromised, especially when the information is stored indefinitely?*

JOHN WOOD ANSWER:

We believe a strong cyber security strategy is at the forefront of maintaining a comprehensive risk management and incident response plan, and that the following steps should be taken to better protect information. An enterprise should first understand the types of data that need to be protected and where that data is located/stored. Second, a company must invest in protection mechanisms that can identify malicious code and irregular network traffic. Third, a healthy response plan and strategy for dealing with potential and actual incidents, breaches or compromises is extremely important. The future of defense must include better tools and processes to quickly uncover malicious code or Advanced Persistent Threats (APTs), and quickly recover from a compromise or breach. Fourth, an entire process for "watching the watchers" and thus continuously vetting/validating the insider threat is needed. Finally, the sharing of threat data throughout the organization's specific community of interest should be embraced.

To these steps, I would add that continually testing and refining information security policies and practices may ultimately be the largest contributor to long-term success in defending a network against attack or compromise. This is not only because of evolving threats, but also because as networks evolve, each iteration adds vulnerability. Finally, contrary to what some believe, networks are not, and should not be, "flat" or static, and they are never the same from one organization to another. Protections associated with defending data sets should be specific to the environment and the data being protected. There are no short cuts or "panacea products."

REP. LOUDERMILK QUESTION # 2A - *How much do you estimate that it could cost to ensure the system is sufficiently protected against evolving cyber threats?*

JOHN WOOD ANSWER:

Consistent with the point I made above -- that all networks are not the same and different organizations and agencies face different threat situations and environments -- this cannot be answered without a very thorough analysis of each specific system in question. It's not just as simple as spending a predetermined amount of money to buy a product/tool -- it's about spending the necessary money to buy the *right* product(s) to fit the specific need. Each system is different, so it's not possible to say how much should be spent by a given entity without them doing their own due diligence.

REP. GARY PALMER QUESTION - *What percentage of cyberattacks are the result of an inside job or are conducted with the aid of someone on the inside?*

JOHN WOOD ANSWER:

The 2015 Clearswift Insider Threat Index (U.S. edition) released in November found that nearly three-quarters of the breaches (74%) originated from within the extended enterprise, which includes employees, suppliers and former employees. Even when you exclude suppliers (22%) and ex-employees (12%) and consider only breaches originating from the actions of current employees, that's still 40% of all breaches.

Insiders who attempt to sabotage operations or commit fraud often tip their hands in advance of an attack. An individual's cyber-related activities (e.g., deviations from normal or expected behavior on a company's network) are only one piece of the puzzle. Network activity, criminal data, social media/Internet activity (including "deep web" visits, blog entries and use of "dark web" anonymity tools) should be continuously monitored, as well as compliance with corporate/agency-identified policies and security parameters. All data gathered should then be aggregated and reported to authorized company or agency representatives, who can holistically analyze the information and take appropriate action to stay well ahead of potential bad actors.

Responses by Dr. Martin Casado

RESPONSE TO QUESTION FOR THE RECORD TO
The Honorable Gary Palmer (R-AL)
U.S. House Committee on Science, Space, and Technology

Cybersecurity: What the Federal Government Can Learn from the Private Sector

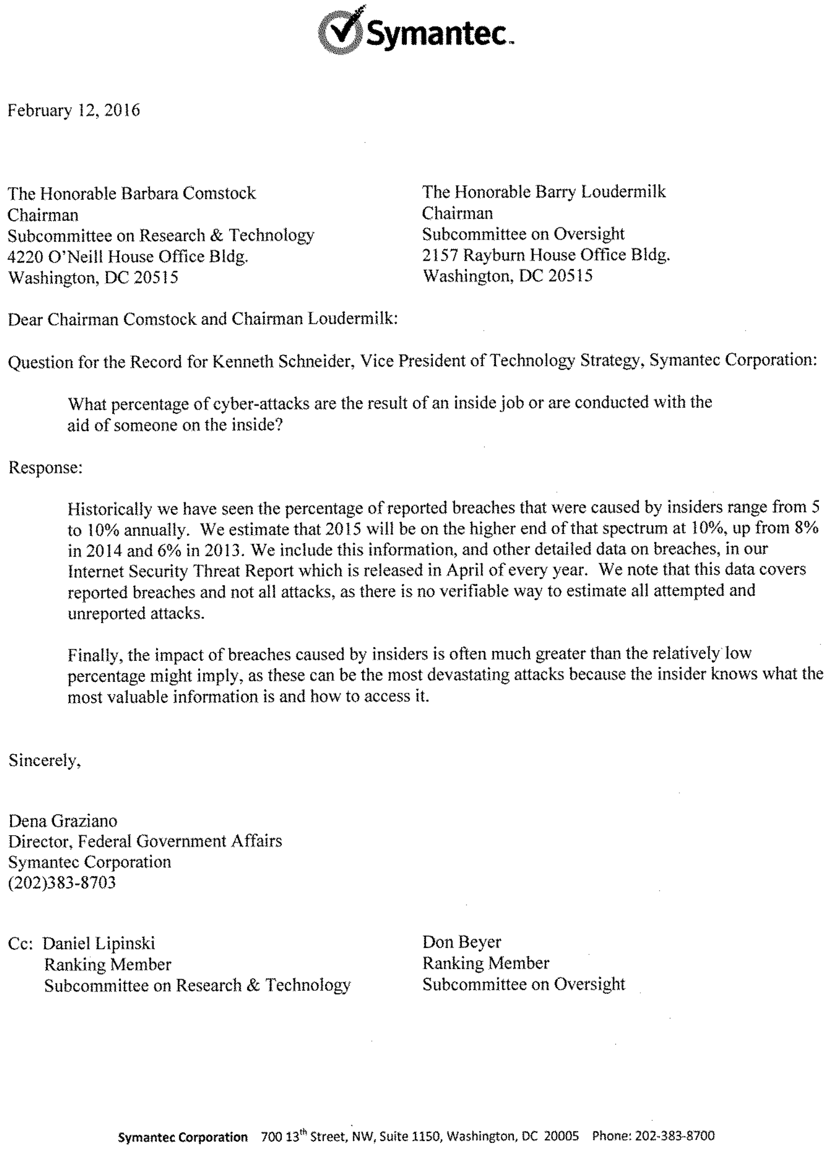
Thursday, August 25, 2016

Dr. Martin Casado, Senior Vice President and General Manager, Networking and Security Business Unit, VMWare

1. What percentage of cyber-attacks are the result of an inside job or are conducted with the aid of someone on the inside?

The U.S. State of Cybercrime Survey, conducted by the U.S. Government in conjunction with members of the private sector, researches Cybersecurity insider threats annually. As of 2014, 28% of electronic crime events are suspected or are known to be caused by inside sources. Additionally, 37% of respondents had experienced insider incidents in 2013, and 53% of respondents had experienced insider incidents in 2012.

Responses by Mr. Ken Schneider



Symantec.

February 12, 2016

The Honorable Barbara Comstock	The Honorable Barry Loudermilk
Chairman	Chairman
Subcommittee on Research & Technology	Subcommittee on Oversight
4220 O'Neill House Office Bldg.	2157 Rayburn House Office Bldg.
Washington, DC 20515	Washington, DC 20515

Dear Chairman Comstock and Chairman Loudermilk:

Question for the Record for Kenneth Schneider, Vice President of Technology Strategy, Symantec Corporation:

> What percentage of cyber-attacks are the result of an inside job or are conducted with the aid of someone on the inside?

Response:

> Historically we have seen the percentage of reported breaches that were caused by insiders range from 5 to 10% annually. We estimate that 2015 will be on the higher end of that spectrum at 10%, up from 8% in 2014 and 6% in 2013. We include this information, and other detailed data on breaches, in our Internet Security Threat Report which is released in April of every year. We note that this data covers reported breaches and not all attacks, as there is no verifiable way to estimate all attempted and unreported attacks.
>
> Finally, the impact of breaches caused by insiders is often much greater than the relatively low percentage might imply, as these can be the most devastating attacks because the insider knows what the most valuable information is and how to access it.

Sincerely,

Dena Graziano
Director, Federal Government Affairs
Symantec Corporation
(202)383-8703

Cc: Daniel Lipinski	Don Beyer
Ranking Member	Ranking Member
Subcommittee on Research & Technology	Subcommittee on Oversight

Responses by Mr. Larry Clinton

U.S. House Committee on Science, Space, and Technology

Cybersecurity: What the Federal Government Can Learn from the Private Sector

Responses to Questions for the Record, February 11th, 2016
Mr. Larry Clinton, President and Chief Executive Officer, Internet Security Alliance

The Honorable Barbara Comstock (R-VA):

Do you think that government and private industry should be utilizing offensive tactics as part of their cyber security strategy? In other words, should companies be "bringing the fight to the bad guy" by aiming malware or by launching a denial-of-service attack at the servers of the potential perpetrators?

The consensus of the ISA board is that it is unwise for private sector entities to be engaging in offensive tactics such as aiming malware or by launching a denial-of-service attack at the servers of the potential perpetrators.

There are multiple reasons we think this is a counterproductive strategy. First, you can't really respond in real time enough to prevent the damage. Second, attribution of cyber attacks is notoriously difficult. Knowing that companies are inclined to "hack-back" would provide incentives for the attack community to launch attacks embedded with clever tools to lead the victims toward an innocent organization as the suspected culprit thus creating further disruption and undermining trust in the legitimate community and potentially starting a war with unpredictable consequences Third, launching offensive strikes will divert scarce cyber security expertise from starting a war with unpredictable consequences. Its real objective, safeguarding the company's interests

These concerns would be magnified if we are, as the question suggests going to consider attacking "potential perpetrators.

The Honorable Barry Loudermilk (R-GA):

Given the number of recent and expansive data breaches of government systems, does it concern you that MIDAS is permanently storing personal and sensitive information of all Americans looking for healthcare coverage?

Storing any personally identifiable information (PII) is a concern for us as any level of compromise of such data could then be used to exploit a number of other systems and infrastructure, which could result in the number of breaches rising exponentially. For example, if a person's blood type, pet name, date of birth, known medical conditions were to be compromised, the information could then be utilized to cause irrevocable harm throughout an individual's life. If it is deemed absolutely necessary to store such highly sensitive information, a program and countermeasures of relative scale/size must be in-place to protect the information from being compromised across the data continuum (at rest, in motion, in use) and across strategic, operational and technical layers of an organization, greatly containing an adversary's ability to navigate beyond the compromised system.

Given the constantly evolving nature of cyber security threats, what steps would your company take to ensure that personally identifiable information is not compromised, especially when the information is stored indefinitely?

Currently encryption and/or non-internet connected systems is really the only way to properly protect PII.

Longer term, technology innovation, and the complimentary cyber security and privacy programs, need to be a top priority as we embrace the digitization of information. A risk-based approach is critical to implementing comprehensive cybersecurity and privacy programs that are proportional to the business model and the evolving cyber threats, vulnerabilities, risks, impact and likelihood we are facing.

How much do you estimate that it could cost to ensure the system is sufficiently protected against evolving cyber threats?

There is simply no way to estimate these costs as we have no way of knowing what the evolution of technology or the threats of that technology will be.

That being said, cost must be a key factor in creating policies aimed at creating a sustainably secure cyber system. Taking a risk management approach inherently means weighing costs and benefits. Industry must take costs into account when assessing all risk decisions as failing to do so would violate the fiduciary duty of a board of directors and undermine the long term viability of the organization.

Government must to a better job of integrating cost into their cyber security programs for themselves and especially those aimed at the private sector. For example, notwithstanding the clear directive of Presidential Executive Order 13636 to make the NIST Cyber Security Framework cost effective there has been no effort to even begin such an analysis now 3 years past the release of the Order.

As a result we have no objective evidence to demonstrate that the Framework is effective in changing cyber security behavior, no objective measurement of what elements of the Framework are cost effective for various industry sectors and sizes and no objective evidence of what elements of the Framework are effective in improving security but are not cost effective (and therefor might merit being incentivized in the interests of national security)

The Honorable Gary Palmer (R-AL):

What percentage of cyber-attacks are the result of an inside job or are conducted with the aid of someone on the inside?

There has been a fair amount of research on this topic however it is difficult to find a clear percentage for various factors such as varying definitions of what counts as an "Insider" and the difference between mistakes leading to vulnerabilities and purposeful malfeasance by an insider.

However, there is a broad consensus that insider attacks are the largest single avenue for cyber incursions.

This highlights the need to consider cyber security as far more than a technical issue to be combatted with standards and technical frameworks (although these are critical elements of a secure cyber system). Cyber security is not an "IT" problem, it is an enterprise wide risk management problem that must be approached, by both government and industry in a multi-faceted risk management approach that includes technology but also embraces human resources, economics, partnerships and senior leadership.

Appendix II

Additional Material for the Record

STATEMENT SUBMITTED BY COMMITTEE RANKING MEMBER EDDIE BERNICE JOHSNON

OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
Subcommittee on Oversight
"Cyber Security: What the Federal Government Can Learn from the Private Sector"
January 8, 2016

Thank you Chairwoman Comstock, Chairman Loudermilk, and Ranking Members Lipinski and Beyer for holding this hearing. This is such an important topic, and one on which our Committee has played an important role. We've developed and enacted some very good bipartisan cybersecurity legislation in this Committee, but our work continues.

It remains an ongoing challenge for us to secure cyberspace for the benefit of our national security and economy, as well as ensuring individual security and privacy. As my colleagues have already noted, protecting our massive stores of information of all types will continue to require the collaborative efforts of the private sector, government, researchers, and the general public. No government agency, no business, and no individual is truly immune from these threats.

Today we will hear from some experts in the private sector about best practices and technologies being implemented by companies. I'm interested to hear about what's being learned and implemented in the private sector that may be useful for government agencies as well. And I'm particularly interested to hear about collaborations between the private sector and our government agencies, on both the research and technology side, and in the development of standards and protocols that will help strengthen the security of all information systems. It is clear that learning and sharing of expertise is a two-way street between the public and private sectors.

I want to thank the witnesses for being here this morning. I look forward to the testimony and discussion, and I yield back.