SAM GRAVES, MISSOURI
CHAIRMAN

NYDIA M. VELAZQUEZ, NEW YORK
RANKING MEMBER

Congress of the United States
U.S. House of Representatives
Committee on Small Business
2361 Rayburn House Office Building
Washington, DC 20515–6315

Memorandum

To:	Members, Subcommittee on Healthcare and Technology
From:	Committee Staff
Date:	December 1, 2011
Re:	Hearing: *Cyber Security: Protecting Your Small Business*

The House Small Business Subcommittee on Healthcare and Technology will meet for a hearing titled, *Cyber Security: Protecting Your Small Business.* The hearing is scheduled to begin at 1:00 p.m. on December 1, 2011 in Room 2360 of the Rayburn House Office Building. The hearing will focus on the issues faced by small businesses in combating cyber security threats, including the role of the federal government and best practice solutions. The subcommittee will receive testimony from The Honorable William M. "Mac" Thornberry, United States House of Representatives (TX-13); David Beam, Senior Vice President, North Carolina Electric Membership Corporation, Raleigh, NC, representing the National Rural Electric Cooperative Association; Glenn Strebe, Chief Executive Officer, Air Academy Federal Credit Union, Colorado Springs, CO, representing the National Association of Federal Credit Unions; Phyllis Schneck, Vice President and Chief Technology Officer, McAfee, Inc., Santa Clara, CA; and Michael Kaiser, Executive Director, National Cyber Security Alliance, Washington, DC.

I. Introduction

"Cyber security" is a term used to describe the act of protecting information stored on computers, the internet, and other digital storage devices.[1] In the past two decades, the internet has grown to be an essential part of the U.S. economy, including for small businesses. The movement of information to the global internet has attracted a growing number of cyber attacks from criminals aiming to steal sensitive information. These are both a major threat to the U.S. national security and the economy. The scope and capabilities of these attacks can vary immensely. They can

[1] U.S. COMPUTER EMERGENCY READINESS TEAM, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *available at*: http://www.us-cert.gov/cas/tips/ST04-001.html.

range from an individual hacker stealing financial information to foreign governments engaged in complex cyber espionage. The results of an attack can be catastrophic for small businesses owners, as many are unable to recover from the loss of their intellectual property and resources. In addition, small businesses generally have less capital to purchase computer security hardware and software, fewer staff members to monitor the system, and less time to develop cyber security policies.

The increase in cyber criminal activity has spurred interest among policymakers to develop legislation aimed at protecting the digital infrastructure. This hearing will give Subcommittee Members the opportunity to learn about cyber security issues faced by small business and the impact of certain policy proposals.

II. Growth of the Internet and Electronic Commerce

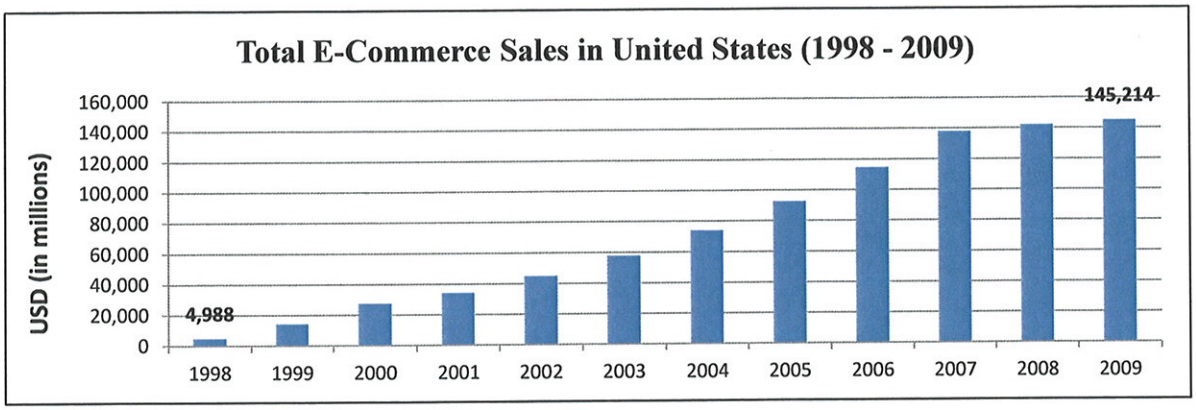
The term "cyberspace" is used to describe the interdependent network of information technology infrastructures that includes the internet, telecommunications networks, and computer systems.[2] Like a chain, the internet is comprised of technology links that are dependent upon each other to function. Components include, but are not limited to, the internet service providers (ISP), website or application hosts, data storage facilities, and the end users. The development and adaption of internet technology continues to grow at a rapid pace. In a recent study, Cisco Systems estimated that global internet traffic will quadruple by 2015.[3]

In the United States, the Federal Communication Commission (FCC) estimates that 97 percent of small businesses use email and online services, and 74 percent have a company website.[4] Along with basic email services, the internet provides a number of tools to help small firms increase their productivity, efficiency, and overall success. Social networking, teleworking, cloud data storage, and global video conferencing are a few examples of opportunities provided by the internet. One of the most important tools is the ability to access to the global electronic marketplace. From 1998 to 2009, electronic commerce in the United States, also known as online sales, grew from $4.9 billion to $145.2 billion, or by 35.9 percent annually.[5]

Figure 1

---

[2] PRESIDENTIAL MEMORANDUM: CYBER SPACE POLICY REVIEW (May 2009), *available at*: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[3] CISCO SYSTEMS, VISUAL NETWORKING INDEX FORECAST, *available at*: http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html#%7Eforecast.
[4] NATIONAL BROADBAND PLAN, FEDERAL COMMUNICATIONS COMMISSION, (2010), *available at*: http://download.broadband.gov/plan/national-broadband-plan.pdf .
[5] BUREAU OF THE CENSUS, UNITED STATES DEPARTMENT OF COMMERCE, RETAIL SALES AND E-COMMERCE-TABLE 1055, *available at*: http://www.census.gov/compendia/statab/cats/wholesale_retail_trade/online_retail_sales.html.



[6]

The continued movement of information and commerce to the internet has attracted a growing number of cyber attacks. Furthermore, the advancements of internet technology has also resulted in more sophisticated attacks.

III. Increased Threat of Cyber Attacks

Targeted cyber attacks are steadily increasing in the United States. As a global leader in producing intellectual property, both private and public institutions will continue to be primary targets for cyber criminals. Some of the key targets include the nation's critical infrastructure,[7] federal and state governments, and private businesses. According to Symantec, 40 percent of all targeted cyber attacks were directed to small businesses with less than 500 employees.[8]

The methods to steal information vary in scope and sophistication. The most common forms of attacks include hacking,[9] malware,[10] physical error, and lost or stolen devices.[11] The expansion of the global network has allowed criminals to conduct these attacks from nearly anywhere in the world. Moreover, many foreign nations are responsible for direct cyber attacks on the United States in an effort to gain intellectual property and economic information. The Office of the National CounterIntelligence Executive released a report on October 11, 2011 stating that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each

---

[6] *Id.*

[7] THE PRESIDENTIAL DECISION DIRECTIVE NO. 63 (PDD-63) (May 1998), *available at*: http://www.justice.gov/criminal/cybercrime/white_pr.htm. PDD-63 first defined critical infrastructure "as those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."

[8] SYMANTEC, TARGETED ATTACKS AND SMBS, *available at*: http://www.symantec.com/connect/blogs/targeted-attacks-and-smbs?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Oct_worldwide_SMBsecurity.

[9] Hacking is generally referred to as gaining access to a computer or server without the owner's permission.

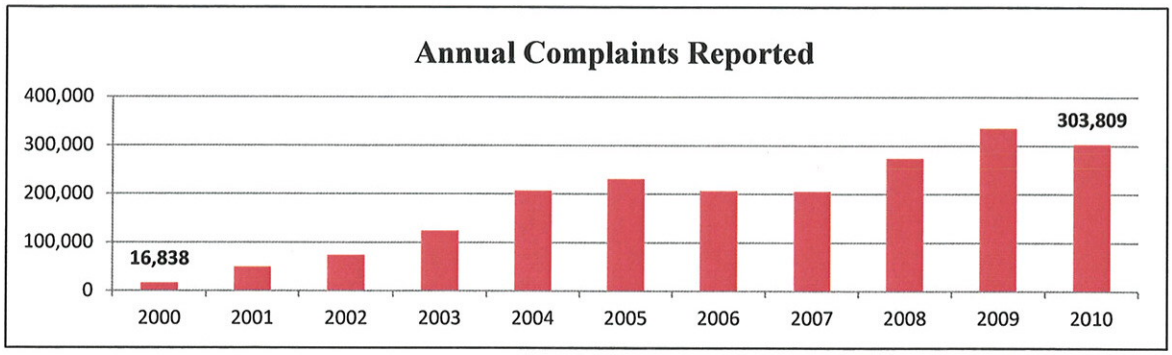
[10] Malware is generally referred to as software or code developed or used for the purpose of compromising or harming information assets without the owner's permission.

[11] VERIZON, 2011 DATA BREACH INVESTIGATIONS REPORT, *available at*: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

year from computer systems in the federal government, corporations and academic institutions. They identified China and Russia as the two largest participants in cyber espionage.[12]

The Internet Crime Complaint Center within the U.S. Department of Justice recorded 303,809 cyber security related complaints in 2010.[13] This is an increase of over 1700 percent from the year 2000 (16,838 reported complaints).[14]

Figure 2



[15]

IV. Key Issues for Small Businesses

Small businesses generally have fewer resources available to combat security threats, which make them an easy target for cyber criminals. In a recent survey, 85 percent of small businesses believe their company is safe from a cyber attack; however the vast majority (77 percent) do not have a formal written security policy in place, and 45 percent surveyed do not provide safety training to their employees.[16]

One cyber attack could be disastrous for a small business. In 2010, the average annual cost of cyber attacks to small and medium sized businesses was $188,242.[17] The statistics also show that nearly 60 percent of small businesses will close within six months after a cyber attack.[18]

---

[12] OFFICE OF NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE, (Oct 2011), *available at*: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[13] INTERNET CRIME COMPLAINT CENTER, 2010 INTERNET CRIME REPORT, *available at*: http://ic3report.nw3c.org/docs/2010_IC3_Report_02_10_11_low_res.pdf.

[14] *Id.*

[15] *Id.*

[16] NATIONAL CYBER SECURITY ALLIANCE, SMALL BUSINESS SURVEY, *available at*: http://staysafeonline.mediaroom.com/index.php?s=43&item=91.

[17] *Id.*

[18] THE CHALLENGES IN DEFENDING AGAINST MALWARE, BUSINESS INSIDER, *available at:* http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9.

In recognition of the threat faced by small businesses, the FCC launched the *Small Biz Cyber Planner* - an online tool that will help small businesses create a customized planning guide against cyber security threats.[19]

V. Federal Government's Efforts in Cyber Security

The federal government has enacted a variety of laws, policies, and tools to assist in the coordination of cyber security among public and private entities. The issue is extremely broad and complex and a number of federal agencies have specific regulations in place around cyber security and information sharing.

In May 1998, President Clinton issued Presidential Decision Directive No. 63 (PDD-63) outlining the federal government's approach to protecting the critical infrastructure against cyber attacks.[20] The directive also established the Information Sharing and Analysis Center, aimed at informing government and private owners of critical infrastructure of cyber threats.[21] In November 2002, President Bush signed the Homeland Security Act of 2002, officially establishing the Department of Homeland Security (DHS).[22] One provision in the Act required DHS to develop a national strategy to protect against cyber attacks and recommend best practices to protect the critical infrastructure.[23] In December 2003, President Bush issued the Homeland Security Presidential Directive 7 (HSPD-7), which designated DHS as the primary agency responsible for cyber security.[24] It also established specific roles for federal agencies to work with the private sector on identifying and communicating threats.[25] In 2006, DHS issued the National Infrastructure Protection Plan, which provided the framework for government and private industries to help protect against cyber attacks.[26] This plan was updated in 2009.[27]

Within DHS, the Office of Cybersecurity and Communications (CS&C) is the primary agency responsible for "assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure."[28] CS&C actively engages with the private sector to educate and coordinate efforts on the best ways to protect against a cyber attack.[29] They administer the

---

[19] FEDERAL COMMUNICATIONS COMMISSION, SMALL BUSINESS CYBER PLANNER, (2011), *available at*: http://www.fcc.gov/document/genachowski-small-biz-cyber-planner.
[20] PRESIDENTIAL DECISION DIRECTIVE NO. 63 (May 1998), *available at*: http://www.justice.gov/criminal/cybercrime/white_pr.htm.
[21] *Id.*
[22] HOMELAND SECURITY ACT OF 2002 (P.L. 107-296, 116 § 2135), *available at*: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf.
[23] *Id.*
[24] HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7 (Dec 2003), *available at*: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.
[25] *Id.*
[26] NATIONAL INFRASTRUCTURE PROTECTION PLAN, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *available at*: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
[27] *Id.*
[28] NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, UNITED STANITED STATES DEPARTMENT OF HOMELAND SECURITY, *available at*: http://www.dhs.gov/xabout/structure/editorial_0794.shtm.
[29] *Id.*

Critical Infrastructure Partnership Advisory Council (CIPAC) that consists of 19 sector specific advisory councils composed of both government and private sector experts.[30] Moreover, CS&C operates the United States Computer Emergency Readiness Team (US-CERT). US-CERT is responsible for analyzing and reducing cyber threats, while also communicating warning information and coordinating incident response activities.[31] US-CERT also conducts voluntary assessments of companies' cyber security policies and procedures.[32]

VI. Current Policy Proposals

There is a strong bipartisan commitment from both chambers of Congress and the President to update certain U.S. laws related to cyber security. There is a broad array of legislation introduced aimed at enhancing some part of the cyber security process. Some of the issues being addressed include data security, reporting requirements, increased law enforcement, harmonized regulations, and education outreach. The most controversial issues involve the appropriate role of the federal government in working with private industry to protect U.S. critical infrastructure.

In 2009, President Obama issued the Cyberspace Policy Review,[33] which served as the framework for a legislative proposal that the Administration submitted to Congress in May 2011.[34] The comprehensive plan contains a broad scope of recommendations including: updating law enforcements provisions;[35] harmonizing state data breach notifications; updating the specific role of DHS; and establishing a process to designate critical infrastructure entities.[36]

On October 5, 2011, the House Republican Cybersecurity Task Force, established by the Speaker of the House, led by Congressman William "Mac" Thornberry (R-TX), released its recommendations for cyber security legislation.[37] The framework focused around four issue areas: 1) critical infrastructure and incentives; 2) information sharing and public private partnerships; 3) updates to existing cyber security laws; and 4) legal authorities.[38] The plan recommends strengthening the role of public-private partnerships, reducing regulatory burden,

---

[30] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, ABOUT CIPAC, *available at*: http://www.dhs.gov/files/committees/editorial_0843.shtm.
[31] NATIONAL CYBER SECURITY DIVISION, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *available at*: http://www.dhs.gov/xabout/structure/editorial_0839.shtm.
[32] CERT, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, *available at*: http://www.us-cert.gov/control_systems/cstraining.html.
[33] PRESIDENTIAL MEMORANDUM: CYBER SPACE POLICY REVIEW (May 2009), *available at*: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
[34] PRESIDENT MEMORANDUM: CYBERSECURITY LEGISLATIVE PROPOSAL (May 2011), *available at:* http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[36] *Id.*
[37] HOUSE CYBER SECURITY TASK FORCE RECOMMENDATIONS (October 2011), *available at*: http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf.
[38] *Id.*

and creating voluntary incentives for the private sector to protect against cyber attacks.[39] It also recognizes that there is no one-size-fits-all approach to cyber security, and recommends that the committees of jurisdiction mark up individual bills.

Earlier this year, Congresswoman Mary Bono Mack (R-CA) introduced the Secure and Fortify Data Act (H.R. 2577), which establishes national standards for responding to a breach in data security.[40] This legislation will require those holding sensitive information from a third party to develop policies and procedures to ensure property security; and also require notification to the Federal Trade Commission (FTC) within 48 hours of a reported breach.[41]

In the Senate, Majority Leader Harry Reid has organized bipartisan, cross-committee working groups to reconcile multiple proposals into a broad comprehensive cyber security bill, which is still being drafted. Reid stated his intention to take up the comprehensive bill early in 2012.[42]

VII. Conclusion

The threat of a cyber attack on a small business could be catastrophic. Unlike large corporations, small businesses do not have the resources and capabilities to combat sophisticated cyber attacks. In reviewing legislation, policy makers should understand there is not a one-size-fits-all approach for cyber security; as small businesses are unable to handle the increased regulatory burden.

---

[39] *Id.*
[40] H.R. 2577, 112th Cong. (2011).
[41] *Id.*
[42] Gautham Nagesh, *Reid Says Senate Will TakeUp Cybersecurity Bill Next Year*, THE HILL, November 17, 2011, *available at*: http://thehill.com/blogs/hillicon-valley/technology/194245-senate-will-take-up-cybersecurity-bill-next-year.