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: March 19, 2013
Re: Hearing: Protecting Small Businesses Against Emerging and Complex Cyber-Attacks

---

The Subcommittee on Health and Technology of the Committee on Small Business will meet for a hearing titled, Protecting Small Businesses Against Emerging and Complex Cyber-Attacks. The hearing is scheduled to begin at 10:00 a.m. on March 21, 2013 in Room 2360 of the Rayburn House Office Building. The hearing will examine the increased volume and complexity of cyber-attacks as they affect emerging technologies utilized by small businesses. As new technologies are deployed, additional opportunities exist for cyber-criminals to attack firms and steal their valuable information.

I. Background

The Internet has the potential to transform the way small businesses operate and compete in the 21st Century. Along with basic email services, advanced telecommunications technology provides a number of tools to help small firms increase their productivity, efficiency, and overall success. These include social media, mobile services, cloud data storage, and global video conferencing. However, the movement of information from paper to electrons has attracted a growing number of criminals aiming to steal sensitive and valuable information through attacks on computer systems, called cyber-attacks.

Cyber-attacks are a major threat to both the United States' national security and the economy. The scope and capabilities of these attacks can vary immensely; they can 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 their systems, 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 and individuals' information. This hearing will provide Subcommittee members the opportunity to understand the rapid growth of

Internet technology available to small firms, and to examine the increased threat and complexity of cyber-attacks on small businesses.

II. Growth of the Internet and Information Technology (IT)

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. Collectively, the hardware and software that support these components are referred to as IT.

The development and adoption of these technologies and the Internet continue to grow at a rapid pace. In a recent study, Cisco Systems stated that global Internet traffic has increased eightfold over the past five years, and will grow at a compound annual growth rate of 29 percent from 2011 to 2016.[1]

The Internet is also of growing importance for small businesses. 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.[2] The Internet provides the opportunity for small businesses to utilize a variety of tools to increase productivity, reduce costs, increase sales, and increase their overall efficiency.

One of the most important tools the Internet offers to businesses is the ability to access the global electronic marketplace. According to the latest data, electronic commerce in the United States, also known as online sales, reached $169 billion in 2010, which represents a nearly 3500 percent increase from $4.9 billion registered in 1998.[3] The Internet also has generated an entrepreneurship boom of businesses developing innovative technologies and new capabilities, such as cloud computing and mobile applications.

Cloud Computing

The term "cloud computing" is defined by the National Institute of Standards and Technology (NIST) as a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly released with minimal effort or interaction from the service provider.[4] For small businesses, cloud computing provides an opportunity to shift many of their information technology services (such as data storage, software, and security) to a cloud provider, instead of purchasing and managing the necessary IT on-site. This could result in

[1] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html.

[2] NATIONAL BROADBAND PLAN, FEDERAL COMMUNICATIONS COMMISSION 16 (2010), *available at* http://download.broadband.gov/plan/national-broadband-plan.pdf.

[3] BUREAU OF THE CENSUS, UNITED STATES DEPARTMENT OF COMMERCE, MEASURING THE ELECTRONIC ECONOMY-TABLE 5, *available at* http://www.census.gov/econ/estats/2010/all2010tables.html.

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, UNITED STATES DEPARTMENT OF COMMERCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

substantial savings for small businesses.[5] However, the centralization of sensitive information to cloud computing data warehouses has made them a growing target for cyber-attacks.

Mobile Applications

The rapid growth of wireless smartphones and tablets has led to the innovation of mobile software applications. Mobile applications allow businesses and consumers to share information and communicate by a touch of a button on their mobile device. Smart phone and tablet manufacturers have reported that there are over 700,000 different applications available to be downloaded on their devices.[6] There are a variety of mobile applications that increase productivity and efficiency of small businesses, including mobile banking and social media.[7] This new development could be another avenue for potential cyber-hackers to steal information.[8]

Given the evident benefits, it is not surprising that small businesses have reported the Internet to be an essential component for their continued growth and success.[9] However, the continued movement of information and commerce to the Internet has attracted a growing number of cyber-attacks. Moreover, these cyber-thieves are also utilizing new technology to develop more sophisticated attacks on small businesses.

III. Increased Threat of Cyber-Attacks

Targeted cyber-attacks are steadily increasing in the United States. As a global leader in producing intellectual property, America's private and public institutions will continue to be primary targets for cyber-criminals. The Internet Crime Complaint Center within the United States Department of Justice recorded 314,246 cyber-security related complaints in 2011.[10] This is an increase of over 1700 percent from the year 2000 (16,838 reported complaints).[11] Some of the key targets include the nation's critical infrastructure,[12] federal and state governments, and

[5] Cicely K. Dyson, *Can the Cloud Help Small Businesses?,* WALL ST. J., January 9, 2013, *available at* http://online.wsj.com/article/SB10001424127887323706704578230641145851624.html.

[6] Jessica E. Lessin and Spencer E. Ante, *Apps Rocket Toward $25 Billion in Sales*, THE WALL ST. J., March 4, 2013, *available at* http://online.wsj.com/article/SB10001424127887323293704578334401534217878.html.

[7] For example, mobile banking applications allow small businesses to expedite the processing of payments between customers, vendors, and financial institutions from a mobile device. Social media mobile applications, like Facebook and Twitter, provide an online platform for small businesses to communicate their marketing and branding messages from mobile phones and tablets to consumers who also have such devices.

[8] MCAFEE, 2013 THREATS PREDICTION 4 (2013), *available at* http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.

[9] SMALL BUSINESS ADMINISTRATION, OFFICE OF ADVOCACY, THE IMPACT OF BROADBAND SPEED AND PRICE ON SMALL BUSINESS at 50 (2010), *available at* http://www.sba.gov/sites/default/files/rs373tot_0.pdf.

[10] INTERNET CRIME COMPLAINT CENTER, 2011 INTERNET CRIME REPORT 6, *available at* http://www.ic3.gov/media/annualreport/2011_ic3report.pdf.

[11] *Id.*

[12] The term "critical infrastructure" is defined 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." THE PRESIDENTIAL DECISION DIRECTIVE NO. 63 (PDD-63) (May 1998), *available at* http://www.justice.gov/criminal/cybercrime/white_pr.htm.

private businesses. According to Symantec, 18 percent of all targeted cyber-attacks were directed to small businesses with less than 250 employees.[13]

The methods to steal information vary in scope and sophistication. The most common forms of attacks include hacking,[14] malware,[15] physical error, and lost or stolen devices.[16] The expansion of global communications technology, such as the Internet, allows 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 Counter Intelligence 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 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.[17]

IV. Key Issues and Best Practices 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, 77 percent of small businesses believe their company is safe from a cyber-attack; however the vast majority (87 percent) do not have a formal written security policy in place, and 60 percent surveyed do not have a privacy policy in place to protect company information.[18] To help small businesses be better prepared, the FCC launched the *Small Biz Cyber Planner* - an online tool to help small businesses create a customized plan guide against cyber-threats.[19]

Even 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.[20] Some statistics show that nearly 60 percent of small businesses will close within six months after a cyber-attack.[21]

V. Federal Government's Efforts to Prevent Cyber-Attacks and Protect IT

Since President Clinton's 1998 directive (PDD-63),[22] the federal government has taken an increasingly active role in protecting critical infrastructure and preventing cyber-attacks. The most recent efforts are encapsulated in the Department of Homeland Security's (DHS) National

[13] SYMANTEC, INTERNET SECURITY THREATS 2011 at 12, *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

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

[15] 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.

[16] *Id.* at 12-13.

[17] OFFICE OF NATIONAL COUNTER INTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 4 (Oct 2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[18] NATIONAL CYBER SECURITY ALLIANCE, SMALL BUSINESS SURVEY, *available at* http://www.staysafeonline.org/stay-safe-online/resources/.

[19] http://www.fcc.gov/document/genachowski-small-biz-cyber-planner.

[20] *Id.*

[21] http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9.

[22] PRESIDENTIAL DECISION DIRECTIVE NO. 63 (May 1998), *available at* http://www.justice.gov/criminal/cybercrime/white_pr.htm.

Infrastructure Protection Plan (NIPP).[23] In addition to the NIPP, other divisions within DHS, particularly the Office of Cybersecurity and Communications (CSC)[24] and the United States Computer Emergency Readiness Team[25] are tasked with protecting the nation's IT and coordinating these efforts with states, local governments, and private entities.

On February 12, 2013, President Obama issued an Executive Order aimed at improving the critical infrastructure's security against possible cyber-attacks.[26] The order establishes the Department of Homeland Security as having a lead role in cyber-security[27] and encourages the federal government to increase their information sharing with the private-sector entities.[28] The order also directs NIST to develop the framework to reduce cyber-risks to the critical infrastructure, including working with the private sector to develop industry standards and best practices.[29]

VI. Policy Initiatives for the 113th Congress

There is a strong bipartisan commitment from both chambers of Congress and the President to update certain domestic laws related to cyber-security. Recent legislative proposals have addressed data security, stronger federal agency coordination, reporting requirements, increased law enforcement and workforce, and education outreach. The most controversial issues involve the appropriate role of the federal government in working with private industry to protect critical infrastructure.

On February 13, House Intelligence Committee Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger introduced H.R. 624, the Cyber Intelligence and Sharing Protection Act.[30] This legislation would allow the federal government to provide classified cyber-threat information to the private sector to better protect against a possible cyber-attack.[31] The legislation also provides liability protection against companies acting in good faith to protect their network.[32]

On February 15, Homeland Security Committee Chairman Michael McCaul introduced H.R. 765, the Cybersecurity Enhancement Act of 2013. This legislation seeks to improve agency coordination and cooperation regarding cyber-security research and developments.[33] The bill also aims to increase the education, public awareness, and workforce around cyber-threats by coordinating with universities and other public-private organizations.[34]

[23] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN 15-16, available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. The plan was originally issued in 2006 and revised in 2009. *Id.* at 7.

[24] http://www.dhs.gov/xabout/structure/editorial_0794.shtm.

[25] http://www.us-cert.gov/about-us.

[26] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[27] *Id.*at § 4, 78 Fed. Reg. at 11,739.

[28] *Id.*at § 4(e), 78 Fed. Reg. at 11,740.

[29] *Id.* at § 7, 78 Fed. Reg. at 11,740-41.

[30] H.R. 624.

[31] *Id.* at § 1104.

[32] *Id.* at § 1104(b)(4).

[33] H.R. 756.

[34] *Id.* at §§ 105-108.

VII. Conclusion

The Internet and new technology are a key component for small businesses to compete in the 21st Century. However, the movement of information and commerce to the Internet has provided a new opportunity for cyber-criminals aiming to steal sensitive and valuable information from small businesses. Unlike large corporations, small businesses do not have the resources and capabilities to combat sophisticated cyber-attacks. Legislation in this area then must strike a balance between the imposition of overly onerous burdens on small business and the need to protect America's IT.