STEVE CHABOT, OHIO
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, Committee on Small Business
From:	Committee Staff
Date:	April 18, 2016
Re:	Hearing: "Small Business and the Federal Government: How Cyber Attacks Threaten Both"

On Wednesday, April 20, 2016 at 11:00 a.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will hold a hearing to examine the current state of cyber security for small firms and various supporting federal agencies and potential solutions to strengthen their efforts. Information technology provides small businesses with the necessary tools to efficiently engage in the global economy. However, as small businesses increasingly rely on web-based products and services, they face an even greater threat from cyber criminals. Even a simple cyber attack can effectively destroy a small business. Recent studies indicate that cyber security measures continue to be one of the top issues for small businesses. Unfortunately, some analyses have found that not only are many small businesses underprepared to combat cyber attacks, the very federal agencies tasked with supporting small businesses lack essential resources to defend against cyber-criminals.

I. Background

The Internet is altering small business operations and establishing a highly competitive marketplace in the 21st century. 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 digital has resulted in greater opportunities for criminals. The risk of theft and manipulation of sensitive and valuable information has increased significantly. These events are referred to as cyber attacks.

Cyber attacks are a major threat to both the United States' national security and economy. The scope and capabilities of cyber attackers can vary immensely; they are viewed today as "mainly individual hackers with purely malicious intent, or perhaps criminal groups intending to use information networks for profit seeking."[1] However, "actors with political or ideological agendas—including terrorist groups, rogue countries and even big powers such as China and Russia—will also pursue cyber power and will play roles of growing importance."[2] The outcome of an attack can be catastrophic for small business owners because many firms 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 defense strategies.

[1] Richard Krugler, *Deterrence of Cyber Attacks*, at 5, *in* Cyberpower and National Security (Franklin D. Kramer, Stuart H. Starr & Larry Wentz eds. 2009), *available at* http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf.
[2] *Id.*

The increase in cyber criminal activity has spurred interest among policymakers to develop legislation aimed at protecting digital infrastructure and individuals' information. This hearing will provide Committee Members with the opportunity to understand the rapid growth of Internet technology used by small firms, and to examine the increased threat of 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, Internet service providers (ISP), website or application hosts, data storage facilities, and end users. 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 more than five-fold in the past five years and will increase three-fold over the next five years.[3]

The Internet is also of growing importance for small businesses due to it providing opportunities for small businesses to utilize a variety of tools to increase productivity, reduce costs, increase sales, and increase their overall efficiency. This is demonstrated by its ability to give small business access to global markets in a cost effective manner According to the latest data, electronic commerce in the United States, also known as online sales, reached $340.8 billion in 2015,[4] which represents a nearly 6855 percent increase from $4.9 billion registered in 1998.[5] The Internet also has generated an entrepreneurship boom of businesses developing innovative technologies and new capabilities, such as cloud computing and mobile applications.

A. *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."[6] 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. Nearly 80 percent of United States small businesses will be fully adapted to cloud computing by 2020, more than doubling the current 37 percent rate.[7] However, the centralization of sensitive information to cloud computing data warehouses has made them a growing target for cyber attacks.

B. *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. Smart phone and tablet manufacturers have reported that there are over 3 billion different applications available to be downloaded on their mobile devices.[8] There are a

[3] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

[4] BUREAU OF THE CENSUS, U.S. CENSUS BUREAU NEWS (FEBRUARY 2016), *available at* https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[5] BUREAU OF THE CENSUS, MEASURING THE ELECTRONIC ECONOMY TABLE 5 (2010), *available at* http://www.census.gov/econ/estats/2010/all2010tables.html.

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

[7] http://www.intuit.com/company/press-room/press-releases/2014/IntuitStudyShowsHowtheCloudWillTransformSmallBusinessby2020/.

[8] *Modern Tools in a Modern World: How App Technology is Benefitting Small Businesses*, 114th Cong. (2015) (statement of Morgan Reed at 2, Executive Director, ACT | The App Association), *available at* http://smbiz.house.gov/uploadedfiles/7-23-2015_morgan_reed_written_testimony.pdf.

variety of mobile applications that increase productivity and efficiency of small businesses, including mobile banking and social media.[9] Mobile applications could be another avenue for potential cyber hackers to steal information.[10]

Given the evident benefits, it is not surprising that small businesses have reported an increase in utilization of technology, and, specifically, newer technology platforms such as cloud computing, smart phones, tablets, and high-speed internet options.[11] 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 269,422 cyber security related complaints in its 2014 report.[12] This is an increase of over 1500 percent from the year 2000 (16,838 reported complaints).[13] Some of the key targets include the nation's critical infrastructure,[14] federal and state governments, and private businesses. According to a report by Verizon Enterprise, 71 percent of cyber attacks occurred in businesses with fewer than 100 employees.[15]

The methods to steal information vary in scope and sophistication. The most common forms of attacks include hacking,[16] malware,[17] physical error, and lost or stolen devices.[18] 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.[19]

[9] 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.

[10] MCAFEE, 2015 THREATS PREDICTION (2015), *available at* http://www.mcafee.com/us/security-awareness/articles/mcafee-labs-threats-predictions-2015.aspx.

[11] NATIONAL SMALL BUSINESS ASSOCIATION, 2013 SMALL BUSINESS TECHNOLOGY SURVEY 6 (2013), *available at* http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf.

[12] INTERNET CRIME COMPLAINT CENTER, 2014 INTERNET CRIME REPORT 6, *available at* http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

[13] *Id.*

[14] 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." Presidential Decision Directive No. 63, at PDD-63 (1998), *reprinted in* National Telecommunications and Information Administration, Notice, 63 Fed. Reg. 41, 804 (Aug. 5, 1998).

[15] VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT at 9 [hereinafter Verizon], *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[16] Hacking is generally referred to as the act of an unauthorized user attempting to or gaining access to an information system. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[17] Malware is generally referred to as software that compromises the operation of a system by performing an unauthorized function or process, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[18]Verizon, *supra* note 15, at 12-13.

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

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

Since President Clinton's 1998 directive (PDD-63), 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 Infrastructure Protection Plan (NIPP).[20] In addition to the NIPP, other divisions within DHS, particularly the Office of Cybersecurity and Communications (CSC)[21] and the United States Computer Emergency Readiness Team[22] 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.[23] The order established DHS as having a lead role in cyber security[24] and encouraged the federal government to increase their information sharing with the private-sector entities.[25] The order also directed 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.[26] The NIST Cybersecurity Framework Version 1.0 was released on February 12, 2014.[27] NIST held a Cybersecurity Framework Workshop in April 2016 to develop future versions of the Cybersecurity Framework.

V. Cyber Attacks on Federal Agencies and Implications for Small Businesses

Nearly every federal agency has some level of engagement with small businesses; for example, United States federal agencies provide services to small businesses, hire small businesses for government contracts, and process financial and personal information. A cyber attack on a federal agency that interacts with small businesses could have a devastating impact.

Last year, the Internal Revenue Service (IRS) was victim of a major cyber attack and they are now reporting the attackers stole over 700,000 taxpayers' data.[28] In February, the IRS announced that the hackers were "using personal data stolen elsewhere outside the IRS, identity thieves used malware in an attempt to generate E-file PINs[29] for stolen Social Security numbers."[30]

Furthermore, in March 2016, the IRS temporarily suspended the Identity Protection Personal Identification Number (IP PIN)[31] in an effort to review the IP PIN service to identify any additional weaknesses in the system before resuming service.[32] Yet, an April 2016 Government Accountability Office (GAO) report found that the IRS paid an estimated $3.1 billion in fraudulent IDT returns[33] and that "while the IRS had made progress in implementing information security controls, it needs to continue to

[20] DHS, 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.
[21] http://www.dhs.gov/xabout/structure/editorial_0794.shtm.
[22] http://www.us-cert.gov/about-us.
[23] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[24] *Id.* at § 4, 78 Fed. Reg. at 11,739.
[25] *Id.* at § 4(e), 78 Fed. Reg. at 11,740.
[26] *Id.* at § 7, 78 Fed. Reg. at 11,740-41.
[27] NIST, CYBERSECURITY FRAMEWORK VERSION 1.0 (2012), *available at* http://www.nist.gov/cyberframework/.
[28] http://fortune.com/2016/04/16/irs-progress-on-cybersecurity/.
[29] An E-file pin is used in some instances to electronically file a tax return.
[30] https://www.irs.gov/uac/Newsroom/IRS-Statement-on-Efiling-PIN.
[31] According to the IRS, IP PIN is a single-use identification number provided to taxpayers who are victims of identity theft to help prevent future identity theft refund (IDT) fraud because once issued, the IP PIN must accompany their electronically filed tax return or else IRS will reject the return. If a paper return has a missing or incorrect IP PIN, IRS delays processing the return while the agency determines if it was filed by the legitimate taxpayer.
[32] GOVERNMENT ACCOUNTABILITY OFFICE (GAO), INFORMATION SECURITY, IRS NEEDS TO FURTHER IMPROVE CONTROLS OVER TAXPAYER DATA AND CONTINUE TO COMBAT IDENTITY THEFT REFUND FRAUD 4 (2016) (GAO-16-589T), *available at* http://www.gao.gov/assets/680/676097.pdf.
[33] *Id* at 10.

address weaknesses."[34] The recent cyber attacks involving public-facing applications have highlighted the cyber security risks the IRS and the public continue to be exposed to and the need to implement systems that protect sensitive taxpayer data.[35]

In addition to cyber security weaknesses at the IRS, other federal agencies tasked with protecting and supporting small businesses are at risk. An October 2014 investigation conducted by the Small Business Administration (SBA) Office of the Inspector General (OIG) found that the SBA is challenged by long-standing security weaknesses identified in 35 open information technology audit recommendations.[36] Specifically, "the SBA's system software controls have 6 open recommendations averaging more than 700 days past their original target corrective action date."[37] The OIG observed that the SBA continues to face significant security vulnerabilities, including establishing baseline configurations of the SBA's IT platforms.[38]

Moreover, in January 2016, the GAO testified before the Committee on Small Business that "contrary to OMB guidance SBA has not conducted regular reviews of its operational IT investments to ensure that they continue to meet agency needs."[39] GAO also noted that the SBA is currently unable to confirm that its IT investments are cost-effective, meeting agency goals or are being effectively managed.[40]

VI. Key Issues and Best Practices for Small Businesses

The government efforts to counter cyber attacks are vital to protect critical infrastructure. However, government sharing of information still requires implementation activities by the private sector. Small businesses generally have fewer resources available to combat security threats, which make them an easy target for cyber criminals. In a recent survey, 81 percent of small businesses are concerned about a cyber attack; 63 percent have cyber security measures in place, and 71 percent of small businesses received a phishing email.[41] 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 to guide against cyber threats.[42]

Protective activities (such as those offered by the FCC) are particularly important to small business; even one cyber attack could be disastrous for a small business. In a 2014 survey, the average cost of a cyber attack on a small business was $32,020.56.[43] Some statistics show that nearly 60 percent of small businesses will close within six months after a cyber attack.[44]

VII. Policy Initiatives for the 114th 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,

[34] *Id* at 17.
[35] *Id.*
[36] SBA, REPORT ON THE MOST SERIOUS MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE SMALL BUSINESS ADMINISTRATION IN FISCAL YEAR 2015 2 (2014) (REPORT NUMBER 15-01), *available at* https://www.sba.gov/sites/default/files/oig/SBA%20OIG%20Report%2015-01%20-%20FY%202015%20Management%20Challenges_0.pdf.
[37] *Id.*
[38] *Id.*
[39] *Attention Needed: Mismanagement at the SBA – The GAO Findings*, 114th Cong. (2016) (statement of William B. Shear at 9, Director, Financial Markets and Community Investment, United States Government Accountability Office), *available at* http://smbiz.house.gov/uploadedfiles/1-06-2016_shear_testimony.pdf.
[40] *Id.*
[41] http://www.nationalcybersecurityinstitute.org/small-business/business-cybersecurity-statistics/.
[42] http://www.fcc.gov/document/genachowski-small-biz-cyber-planner.
[43] NSBA, 2015 YEAR-END ECONOMIC REPORT, *available at* http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
[44] http://www.businessinsider.com/the-challenges-in-defending-against-malware-2011-9.

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 January 8, 2015, House Intelligence Committee Ranking Member C.A. Dutch Ruppersberger introduced the Cyber Intelligence and Sharing Protection Act.[45] 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.[46] H.R. 234 also provides liability protection against companies acting in good faith to protect their network.[47]

On April 13, 2015 House Homeland Security Committee Chairman Michael McCaul introduced the National Cybersecurity Protection Advancement Act of 2015.[48] This legislation seeks to strengthen the National Cybersecurity and Communications Integration Center's role as the lead civilian interface for the sharing of cyber-security risks and incidents.[49] It also aims to preserve existing public-private partnerships to ensure ongoing collaboration on cyber security.[50] The National Cybersecurity Protection Advancement Act of 2015 passed the House on April 23, 2015.[51] It is awaiting action in the Senate.

VIII. 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. Cyber security must be made a priority for small businesses, as well as the federal agencies that work with them. There must also be a balance between the imposition of overly onerous burdens on small business and the need to protect America's IT.

[45] H.R. 234, 114th Cong., 1st Sess. (2015)
[46] *Id.* at § 1104.
[47] *Id.* at § 1104(b)(4).
[48] http://homeland.house.gov/press-release/mccaul-ratcliffe-introduce-pro-privacy-pro-security-cybersecurity-bill-committee.
[49] *Id.*
[50] *Id.*
[51] H.R. 1731, 114st Cong., 1st Sess. (2015)