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: March 6, 2017
Re: Hearing: "Small Business Cybersecurity: Federal Resources and Coordination"

On Wednesday, March 8, 2017 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 how federal agencies are working to coordinate and disseminate cybersecurity[1] resources for small businesses. As small businesses' reliance on information technology products and services grows each year, they face an even greater threat from cyber attacks. Although many federal agencies provide cybersecurity resources for small businesses, there is a lack of coordination between the various agencies to ensure that small businesses can access these tools to protect and combat cyber attacks in an efficient and effective manner. As the Committee has learned through previous hearings, a cyber attack can destroy a small business. This hearing will examine how the federal government can ensure that small businesses have the tools they need to protect themselves from cyber threats.

I. Background

Small businesses are an integral component of the country's cyber infrastructure and the security of their networks and data is a top priority for both public and private sectors. Moreover, the ever changing dynamic of information technology is altering small business operations and establishing a highly competitive marketplace in the 21st century. Advances in technology provide a number of tools to help small firms increase their productivity, efficiency, and overall success. These tools 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 and cyber threats and the risk of theft and manipulation of sensitive and valuable information has increased significantly. These events are referred to as cyber attacks.

[1] Cybersecurity is defined as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity authentication, confidentiality, and nonrepudiation" NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), NIST INTERAGENCY REPORT, SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS, 2 (2016), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

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."[2] American policymakers and federal agencies are aware that a cyber attack on a small business can be detrimental, not only to the business, but to its customers, employees, and business partners.[3] The Small Business Committee has also learned that cyber threats to small businesses are carried out by a wide array of cyber bad actors, including foreign governments that – through subversive tactics – employ state-backed firms to implement and accomplish cyber attacks, cyber espionage, and accomplish other national strategic objectives, making it difficult to identify the responsible entity.[4] 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.

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 288,012 cybersecurity related complaints in its 2014 report.[5] This was an increase of over 1500 percent from the year 2000 (16,838 reported complaints).[6] Some of the key targets included the nation's critical infrastructure,[7] 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.[8]

In recent years, federal agencies have begun offering resources directly to small businesses to ensure they have the necessary tools to develop stronger information security[9] and cybersecurity systems. Furthermore, threats to information technology infrastructure and Americans' information security has spurred interest among policymakers to investigate looming threats and

---

[2] Richard Krugler, *Deterrence of Cyber Attacks* 5, *in* CYBERPOWER AND NATIONAL SECURITY (Franklin D. Kramer ET AL., eds., 2009), *available at* http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-13.pdf.

[3] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[4] As the U.S.-China Commission has highlighted, circumstantial evidence suggests that cyber incidents are state sponsored because the actors typically target key defense and foreign-policy sources, which are more useful to state and not commercial operations. U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2015 ANNUAL REPORT TO CONGRESS 192 (2015), *available at* http://www.uscc.gov/Annual_Reports/2015-annual-report-congress.

[5] INTERNET CRIME COMPLAINT CENTER, 2015 INTERNET CRIME REPORT 4, *available at* https://www.ic3.gov/media/annualreport/2015_IC3Report.pdf .

[6] *Id.*

[7] 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).

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

[9] Information Security is defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." 44 U.S.C. §§ 3552(b)(3), (2014).

develop methods to better protect small businesses from cyber attacks. This hearing will provide Committee Members with the opportunity to learn more about existing federal cybersecurity resources for small businesses and how those resources can be efficiently and effectively disseminated.

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, 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. A recent Cisco Systems study stated that global Internet traffic has increased more than five-fold in the past five years and is expected to increase three-fold over the next five years.[10]

The Internet is also of growing importance for small businesses because it provides opportunities for small businesses with a variety of tools to increase productivity, reduce costs, increase sales, and increase overall efficiency. This is demonstrated by its ability to give small businesses access to global markets in a cost effective manner. According to 2016 Census data, electronic commerce in the United States, also known as online sales, reached $340.8 billion in 2015,[11] a nearly 6855 percent increase from $4.9 billion registered in 1998.[12] 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 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."[13] 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.[14] However, the centralization of sensitive information to cloud computing data warehouses has made them a growing target for cyber attacks.

---

[10] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.
[11] BUREAU OF THE CENSUS, U.S. CENSUS BUREAU NEWS (2016), *available at* https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.
[12] BUREAU OF THE CENSUS, MEASURING THE ELECTRONIC ECONOMY, TABLE 5 (2010), *available at* http://www.census.gov/econ/estats/2010/all2010tables.html.
[13] NIST, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[14] http://www.intuit.com/company/press-room/press-releases/2014/IntuitStudyShowsHowtheCloudWillTransformSmallBusinessby2020/.

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.[15] There are a variety of mobile applications that increase productivity and efficiency of small businesses, including mobile banking and social media.[16] Mobile applications could be another avenue for potential cyber hackers to steal information.[17]

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.[18] Additionally, the continued movement of information and commerce to the Internet has resulted in greater global market integrations and further interdependencies.[19]

III. Federal Cybersecurity Resources for Small Businesses

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[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 cybersecurity[24] and encouraged the federal government to increase their

---

[15] *Modern Tools in a Modern World: How App Technology is Benefitting Small Businesses: Hearing before the H. Comm. on Small Business*, 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.

[16] 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.

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

[18] 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.

[19] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, *Identifying, Understanding, and Analyzing Critical Infrastructure Independencies*, IEEE CONTROL SYSTEMS MAGAZINE, Dec. 2001.

[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. *Id.* at 7.

[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.

information sharing with the private-sector entities.[25] The order also directed NIST to develop a framework to reduce cyber risks to the critical infrastructure.[26] The framework incorporates input from government and private industry to identify specific parameters that would support and simplify processes for "addressing and managing cybersecurity risks in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[27] The framework also enables businesses to implement a set of best practices for assessing cyber threats and reinforcing cybersecurity efforts regardless of their size or sophistication.[28]

To address the growing concern of small business cybersecurity vulnerabilities, NIST also released a guide, "Small Business Information Security: The Fundamentals," as a resource for small business owners with limited cybersecurity training.[29] The guide enables small business owners to take basic steps toward bolstering their business' information security systems. The document not only provides a step-by-step risk assessment procedure to help identify weaknesses in their systems, but also offers worksheets for assessing the information they keep on file.[30] NIST notes that "the guide is based on NIST's Framework for Improving Critical Infrastructure Cybersecurity."[31]

Although NIST has been tasked with developing the overall framework for cybersecurity protocol, other federal agencies offer cybersecurity resources for small businesses. In 2012, the Federal Communications Commission (FCC) re-launched the "Small Biz Cyber Planner 2.0" to assist small businesses in constructing cybersecurity plans. The FCC established the program with input from various federal agencies and private IT and security companies.[32] The FCC's Cyber Planner 2.0 offers small businesses "details about cyber insurance to mitigate interruptions to business and financial loss from cyber attacks, best practices on spyware, including how to avoid advanced versions of spyware and what immediate steps to take in case of infections, and recommendations to install new software systems that enable remote cleaning and tracking of laptops and mobile devices in case of theft."[33]

The Federal Trade Commission (FTC) serves as both a resource for small business cybersecurity concerns and as a primary regulator of cybersecurity best practices. The FTC offers a number of free resources aimed to help small businesses maintain strong cybersecurity plans while meeting the legal requirements for storing sensitive data. Specifically, the FTC offers guides to address data breaches[34] and best practices for protecting consumers' personal information.[35] The FTC is also tasked with preventing the use of "unfair or deceptive acts or practices in or affecting

---

[25] *Id.* at § 4(e), 78 Fed. Reg. at 11,740.
[26] *Id*. at § 7, 78 Fed. Reg. at 11,740-41.
[27] *Id*.
[28] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[29] http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.
[30] The worksheets help identify and prioritize information; develop an inventory; identify threats, vulnerabilities, and the likelihood of an incident; and prioritize mitigation activities.
[31] https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity.
[32] https://www.fcc.gov/news-events/blog/2012/10/17/fcc-releases-small-biz-cyber-planner-20-empower-small-businesses.
[33] *Id*.
[34] https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.
[35] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

commerce"[36] by businesses. Furthermore, in 2015 at the United States Court of Appeals for the Third Circuit Court, the FTC solidified its role as a leading federal regulator of cybersecurity and data breach response.[37] The FTC also regularly issues policy statements and guidance for businesses on data security issues.[38]

However, federal agencies tasked with protecting and supporting small businesses are also 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.[39] Specifically, "the SBA's system software controls have 6 open recommendations averaging more than 700 days past their original target corrective action date."[40] The OIG observed that the SBA continues to face significant security vulnerabilities, including establishing baseline configurations of the SBA's IT platforms.[41]

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."[42] 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.[43] While SBA faces internal IT challenges, it is working with other agencies to provide cybersecurity resources to small businesses.

NIST has developed InfraGard, a co-sponsorship agreement with the SBA and FBI to conduct regional workshops that focus specifically on IT security for small businesses.[44] The workshops provide small businesses access to IT security personnel to provide advice and education on security threats posed to businesses, as well as how to asses vulnerabilities and identify the necessary protections for such threats.[45] InfraGard also emphasizes the importance of information sharing between the federal government – facilitated through the FBI – and private sector entities.[46]

---

[36] Federal Trade Commission Act, 15 U.S.C. §§ 5-45(a).
[37] *FTC v. Wyndham Worldwide Corp.*, 799F.3d236 (3d Cir. 2015).
[38] https://www.ftc.gov/datasecurity.
[39] 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.
[40] *Id.*
[41] *Id.*
[42] *Attention Needed: Mismanagement at the SBA – The GAO Findings: Hearing Before the H. Comm. on Small Business*, 114th Cong. (2016) (statement of William B. Shear, Director, Financial Markets and Community Investment, United States Government Accountability Office), *available at* http://smbiz.house.gov/uploadedfiles/1-06-2016_shear_testimony.pdf.
[43] *Id.*
[44] http://csrc.nist.gov/groups/SMA/sbc/overview.html.
[45] *Id.*
[46] *Id.*

IV. Policy Initiatives and Considerations for the 115th Congress

There is a strong bipartisan commitment from both chambers of Congress and the President to update certain domestic laws related to cybersecurity. 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 January 17, 2017, Representative Daniel M. Donovan (R-NY) introduced H.R. 584, the Cyber Preparedness Act of 2017.[47] This legislation requires the Department of Homeland Security's (DHS's) State, Local, and Regional Fusion Center Initiative to coordinate with the national cybersecurity and communications integration center (NCCIC) to provide state, local, and regional fusion centers with expertise on DHS cybersecurity resources.[48] This bill passed the House on January 31, 2017 and is awaiting action in the Senate.

In the 114th Congress, Representative Richard L. Hanna's (R-NY) legislation, H.R. 5064, the Improving Small Business Cyber Security Act of 2016, was enacted.[49] This law eases the burden on small businesses facing cyber threats by providing access to additional tools, resources, and expertise through existing federal cyber resources. Specifically, it permits the Department of Homeland Security (DHS) and other federal agencies working in coordination with DHS to provide assistance to small businesses through Small Business Development Centers (SBDC). The information and resources distributed by SBDCs will streamline cyber support for small businesses. Additionally, the law requires the SBA and DHS to collaboratively develop a Small Business Development Center Cyber Strategy in consultation with representatives of SBDCs. It amends the Small Business Act and Homeland Security Act to allow SBDCs to offer cyber support to small businesses in accordance with the Cyber Strategy. This strategy will also provide guidance to SBDCs on how best to use existing federal resources to improve cyber support services for small businesses.

V. Conclusion

The Internet and new technology are key components 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 attackers to steal sensitive and valuable information from small businesses. Unlike large corporations, most small businesses do not have the resources to effectively combat cyber attacks. Cybersecurity must be a priority for small businesses, as well as the federal agencies that work with them. Finally, the various federal agencies tasked with providing small businesses with cybersecurity resources must be better coordinated to drive down duplicative resources and processes and more efficiently and effectively support small business cybersecurity efforts.

[47] H.R. 584, 115th Cong., 1st Sess. (2017).
[48] *Id.*
[49] H.R. 5064 was included in the National Defense Authorization Act for Fiscal Year 2017. Pub. L. No. 114-328, §§ 1841-1844 (2016).