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 20515–0315

Memorandum

To: Members, Committee on Small Business
From: Committee Staff
Date: November 13, 2017
Re: Hearing: "Federal Government and Small Businesses: Promoting Greater Information Sharing for Stronger Cybersecurity"

On Wednesday, November 15, 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 can encourage greater information sharing with small businesses and provide timely assistance and resources when a cyber attack on a small business occurs. Additionally, the hearing will examine the policies that discourage small businesses from engaging with federal agencies for cybersecurity assistance.

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 cyber criminals and 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] 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.[2] The Committee on Small Business has learned

---

[1] 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.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf. (last visited Jul. 24, 2017).

that cyber attacks on 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 other national strategic objectives, making it difficult to identify the responsible entity.[3] The outcome of an attack can be catastrophic for small business owners because 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 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 298,728 cybersecurity-related complaints in its 2016 report.[4] There have been steady increases year over year since the year 2000 (3,762,348 total reported complaints).[5] Some of the key targets include the nation's critical infrastructure,[6] federal and state governments, and private businesses. According to a 2012 report by Verizon Enterprise, 71 percent of cyber attacks occurred in businesses with fewer than 100 employees.[7]

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[8] and cybersecurity systems. Furthermore, threats to information technology infrastructure and Americans' information security have spurred interest among policymakers to investigate looming threats and develop methods to better protect small businesses from cyber attacks.

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

A recent Cisco Systems study estimated that global Internet traffic will increase more than threefold over the next five years.[9] The Internet is of growing importance for small

---

[3] 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.

[4] INTERNET CRIME COMPLAINT CENTER, 2016 INTERNET CRIME REPORT 14 (2016), *available at* https://pdf.ic3.gov/2016_IC3Report.pdf.

[5] *Id.*

[6] 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 63 on Critical Infrastructure Protection: Sector Coordinators, 63 Fed. Reg. 41,804 (Aug. 5, 1998).

[7] 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.

[8] 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).

[9] CISCO, CISCO VISUAL NETWORKING INDEX: FORECAST AND METHODOLOGY, *2016-2021*, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html (last visited Jul. 22, 2017).

businesses because it provides opportunities for small businesses 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,[10] a nearly 6855 percent increase from $4.9 billion registered in 1998.[11]

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."[12] 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. Over two-thirds of businesses increased spending on cloud computing services in 2013 and businesses indicate security as a top benefit of using the cloud.[13] 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.[14] There are a variety of mobile applications that increase productivity and efficiency of small businesses, including mobile banking and social media.[15] Mobile applications could be another avenue for potential cyber hackers to steal information.[16]

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

---

[10] BUREAU OF THE CENSUS, U.S. CENSUS BUREAU NEWS (2016), *available at* https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.
[11] BUREAU OF THE CENSUS, MEASURING THE ELECTRONIC ECONOMY, TABLE 5 (2010), *available at* http://www.census.gov/econ/estats/2010/all2010tables.html.
[12] NAT'L INST. OF STD. AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[13] https://clutch.co/cloud/resources/annual-cloud-computing-survey-2017.
[14] *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.
[15] 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.
[16] MCAFEE, 2015 THREATS PREDICTION (2015), *available at* http://www.mcafee.com/us/security-awareness/articles/mcafee-labs-threats-predictions-2015.aspx.

computing, smart phones, tablets, and high-speed internet options.[17] Additionally, the continued movement of information and commerce to the Internet has resulted in greater global market integrations and further interdependencies.[18] The growing cybersecurity risks to small businesses have resulted in a greater need to share cyber threat information between stakeholders.

III. Cybersecurity Information Sharing

As the federal government and private sector continue to take steps to strengthen small business cybersecurity, the lack of information sharing between federal and private partners poses a major hurdle to effectively combatting cyber attacks.

On February 12, 2013, President Obama issued an Executive Order aimed at improving the critical infrastructure's security against possible cyber attacks.[19] The order established the Department of Homeland Security (DHS) as having a lead role in cybersecurity[20] and encouraged the federal government to increase its information sharing with the private-sector entities.[21] The order also directed NIST to develop a framework to reduce cyber risks to the critical infrastructure.[22] 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."[23] 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[24] which leads to simplification of information sharing processes.

In 2009, DHS established the National Cybersecurity and Communications Integration Center (NCCIC) to serve as an integral component of the cybersecurity information sharing infrastructure for public and private sectors.[25] The NCCIC operates as a round the clock operations center for situational awareness, incident response and management of coordination of the Federal government's cyber and communications activities.[26] DHS states that "the NCCIC shares information among public and private sector partners to build awareness of

---

[17] 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.
[18] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, *Identifying, Understanding, and Analyzing Critical Infrastructure Independencies*, IEEE CONTROL SYSTEMS MAGAZINE, Dec. 2001.
[19] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[20] *Id.* at § 4, 78 Fed. Reg. at 11,739.
[21] *Id.* at § 4(e), 78 Fed. Reg. at 11,740.
[22] *Id.* at § 7, 78 Fed. Reg. at 11,740-41.
[23] *Id.*
[24] NAT'L INST. OF STD. AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[25] GOVERNMENT ACCOUNTABILITY OFFICE (GAO), CYBERSECURITY, DHS'S NATIONAL INTEGRATION CENTER GENERALLY PERFORMS REQUIRED FUNCTIONS BUT NEEDS TO EVALUATE ITS ACTIVITIES MORE COMPLETELY 2 (2017) (GAO-17-163), [hereinafter "GAO Cyber"] *available at* http://www.gao.gov/assets/690/682435.pdf.
[26] DEPT. OF HOMELAND SEC., *National Cybersecurity and Communications Integration Center*, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last visited Nov. 13, 2017).

vulnerabilities, incidents, and mitigations."[27] Furthermore, private sector entities can link to the NCCIC for information products, feeds, and services for free.[28] Additionally, DHS works to facilitate greater information sharing through its Cyber Information Sharing and Collaboration Program (CISCP),[29] a program that "provides a platform and a trusted forum for exchanging threat and vulnerability information, governed by a Cooperative Research and Development Agreement[30] between DHS and each CISCP participant.[31]

The DHS's National Protection and Programs Directorate (NPPD) is also working with CISOs, Chief Security Officers (CSOs), and insurers to explore the potential development of a cyber incident data repository that could assist in the identification of emerging cybersecurity best practices across sectors and help stakeholders offer cybersecurity insurance policies that would incentivize businesses for adopting those best practices."[32]

In March 2016, the NPPD sought input from these various stakeholders on the cybersecurity insurance market's potential to encourage businesses to improve their cybersecurity in return for more coverage at more affordable rates by seeking comments on three white papers prepared by NPPD staff.[33] The NPPD's white papers address the critical need for information sharing as a means to create a more robust cybersecurity insurance marketplace and improve enterprise cyber hygiene practices across the public and private sectors.[34]

In May 2017, President Trump signed an Executive Order[35] which directs the federal government to responsibly secure its IT and data and states that agencies must manage their cybersecurity risk according to NIST's Framework for Improving Critical Infrastructure Cybersecurity.[36] A recent article from Business Insurance states that "private companies seeking government contracts will likely be held to the same standards as the agencies they deal with, which will lead to the wider adoption of the cyber security framework proposed by the NIST"[37] and that "increased compliance with NIST will make the framework even more influential in businesses in all sectors of the economy."[38]

Another major component of the government-private sector information sharing platform is the integration of Information Sharing and Analysis Centers (ISACs) and Information Sharing

---

[27] *Id*.
[28] *Id*,
[29] GAO Cyber, *supra* note 25, at 12.
[30] The Cooperative Research and Development Agreement allows participants to gain as-needed access to NCCIC, a mechanism to receive security clearances, and the ability to participate in bi-directional information sharing.
[31] GAO Cyber, *supra* note 25, at 12.
[32] *Id*.
[33] Nat'l Protection and Programs Directorate; Nat'l Protection and Programs Directorate Seeks Comments on Cyber Incident Data Repository White Papers, 81 Fed. Reg. 17,193, 17,194 (Mar. 28, 2017).
[34] DEPT. OF HOMELAND SEC., ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS, *available at* https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers.
[35] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May. 11, 2017).
[36] *Id*.
[37] *Cyber security framework marches forward*, BUSINESS INSURANCE (Jul. 3, 2017), http://www.businessinsurance.com/article/00010101/NEWS06/912314233/Cyber-security-framework-marches-forward.
[38] *Id*.

and Analysis Organizations (ISAOs). ISACs are non-profit, sector-specific organizations comprised of member organizations from various critical infrastructure entities.[39] For example, banks and credit card processors can engage the Financial Services Information and Sharing Analysis Center (FSISAC) to collaborate on critical security threats to the financial services sector to receive information specifically designed to help protect critical systems and assets from physical cyber security threats in an efficient manner.[40] A 2015 Executive Order directing DHS to encourage the development of ISAOs to facilitate and respond to cyber threats to the critical infrastructure in real time[41] was implemented to develop a more efficient means for granting clearances to members of an ISAO and to engage in "continuous, collaborative, and inclusive coordination with ISAOs via the DHS NCCIC."[42]

Finally, NIST has developed InfraGard, a co-sponsorship agreement with the Small Business Administration and the Federal Bureau of Investigations to conduct regional workshops that focus specifically on IT security for small businesses.[43] The workshops provide small businesses with 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.[44] InfraGard also emphasizes the importance of information sharing between the federal government – facilitated through the FBI – and private sector entities.[45]

However, small businesses face significant challenges in partnering with the federal government to participate in cybersecurity information sharing activities as well. DHS recently provided two possible reasons for small businesses' reluctance to engage federal partners, including "lingering questions around potential legal liabilities and concerns about possible privacy and data protection."[46] Specifically, many businesses are concerned about the type of information that would be provided to the federal government if they used information sharing portals.[47]

IV. Policy Initiatives and Considerations for the 115th Congress

There is strong bipartisan commitment from both chambers of Congress and the President to update certain domestic laws related to cybersecurity. The most controversial issues involve the appropriate role of the federal government in working with private industry to protect critical infrastructure.

---

[39] DEPT. OF HOMELAND SEC., *Information Sharing*, https://www.dhs.gov/topic/cybersecurity-information-sharing (last visited Nov. 13, 2017).
[40] https://www.fsisac.com/
[41] Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 6, 2015).
[42] https://www.dhs.gov/isao.
[43] http://csrc.nist.gov/groups/SMA/sbc/overview.html.
[44] *Id*.
[45] *Id*.
[46] *Enrollment for threat sharing program continues to lag*, FEDERAL COMPUTER WEEK (Jan. 17, 2017), https://fcw.com/articles/2017/11/01/cyber-threat-sharing-johnson.aspx.
[47] *Tackling cybersecurity threat information sharing challenges*, CSO ONLINE (Jan. 17, 2017), https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html.

On January 17, 2017, Representative Daniel M. Donovan (R-NY) introduced H.R. 584, the Cyber Preparedness Act of 2017.[48] This legislation would require 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.[49] This bill passed the House on January 31, 2017 and is awaiting action in the Senate.

On July 10, 2017, Chairman Steve Chabot (R-OH) introduced H.R. 3170, the Small Business Development Center Cyber Training Act of 2017.[50] This bill would amend the Small Business Act to require the Small Business Administration (SBA) to establish a program to provide cybersecurity planning assistance to small businesses.[51] A Senate companion bill, S. 1428, Small Business Cyber Training Act of 2017, has been introduced in the Senate.[52]

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.[53] 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 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 also allows 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.

In the 114th Congress, a compromised version of Senator Richard Burr's (R-NC) legislation, S. 754,[54] the Cybersecurity Information Sharing Act (CISA) was included in the Consolidated Appropriations Act of 2015.[55] This law required the Director of National Intelligence, the Department of Justice, and DHS to develop procedures to share cybersecurity threat information with private entities. Among other things, it incentivizes businesses to engage in information sharing practices with the federal government by providing specific liability protection for information sharing activities. This language is an important step forward in encouraging greater small business participation in information sharing.

---

[48] H.R. 584, 115th Cong., 1st Sess. (2017).
[49] *Id*.
[50] H.R. 3170, 115th Cong., 1st Sess. (2017).
[51] *Id*,
[52] S. 1428, 115th Cong., 1st Sess. (2017).
[53] H.R. 5064 was included in the National Defense Authorization Act for Fiscal Year 2017. Pub. L. No. 114-328, §§ 1841-1844 (2016).
[54] S. 754, 114th Cong. (as passed by the Senate on Oct. 27, 2015).

[55] Consolidated Appropriations Act of 2015, P.L. 114-113, 129 Stat. 2242 ("CISA")

V. Conclusion

Information sharing is a key factor in establishing strong cybersecurity for America's small businesses and the federal government offers a number of organizations and structures for receiving cyber threat information. However, due to small businesses' lack of resources and the complex and technical nature of many cybersecurity information sharing services, small businesses have been slow to adopt information sharing practices. Moreover, small businesses remain wary of the potential legal liabilities and privacy concerns related to cybersecurity information sharing.