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: July 24, 2017
Re: Hearing: "Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"

On Wednesday, July 26, 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 cybersecurity insurance solutions can help small businesses recover from a cyber attack. Small businesses rely on information technology more than ever, yet the very tools that make small businesses competitive have also put them in the crosshairs of cyber attackers. As the federal government and private sector continue to work to strengthen small business cybersecurity, a potential option for reducing the impact of a cyber attack on a small business is cybersecurity insurance. The hearing will examine the challenges small businesses face in selecting a cybersecurity insurance policy and the hurdles insurers must overcome to offer viable and comprehensive cybersecurity insurance solutions.

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

[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.

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 also learned 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 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 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 included 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.

---

[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).

[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 No. 63 at PDD-63 (1998), *reprinted in* National Telecommunications and Information Administration, Notice, 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).

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 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 that 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]

---

[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).

[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

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.[17] Additionally, the continued movement of information and commerce to the Internet has resulted in greater global market integrations and further interdependencies.[18] The mounting cyber risks to small businesses have resulted in innovative private sector solutions to help strengthen security systems and defray costs of recovery from cyber attacks.

III. Cybersecurity Insurance and Small Businesses

It has become increasingly evident that no matter how well-protected a small business' information technology system may be, it is practically impossible to be hack-proof. As a result, many corporate executives are giving consideration to cyber insurance policies as part of the solution. The global cyber insurance market is expected to reach $14 billion by 2022, with a compound annual growth rate of nearly 28 percent from 2016 to 2022, according to Allied Market Research.[19]

According to the federal government, cybersecurity insurance is "designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage."[20] Further, the development of a cybersecurity insurance market may decrease the effectiveness of cyber attacks by incentivizing businesses to take greater preventative measures in return for better cyber insurance coverage and encouraging private sector actors to use standardized best practices by basing premiums on a customer's level of self-protection.[21]

Many small businesses lack adequate commercial insurance to provide liability coverage to protect their businesses from injury or property damage.[22] Furthermore, small businesses that do carry coverage are still at significant risk because "commercial lines policies do not cover many of the cyber risks mentioned above…and coverage of these unique cyber risks through insurance requires the purchase of a special cyber liability policy."[23] Yet, insurance underwriters face difficulties in calculating cyber risk due a lack of data and, therefore, many small businesses

---

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.

[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] ALLIED MARKET RESEARCH, CYBER INSURANCE MARKET (2016), *available at* https://www.alliedmarketresearch.com/cyber-insurance-market.

[20] DEPT. OF HOMELAND SEC., *Cybersecurity Insurance*, https://www.dhs.gov/cybersecurity-insurance# (last visited Jul. 24, 2017) [hereinafter "DHS CYBER"].

[21] *Id.*

[22] A Nationwide-sponsored survey found that 66 percent of small businesses do not have business interruption insurance. https://www.nationwide.com/about-us/083115-small-biz-survey.jsp.

[23] NAT'L ASSOC. OF INS. COMMISSIONERS AND THE CENTER FOR INS. POLICY AND RESEARCH, *Cybersecurity*, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (last visited Jul. 22, 2017), [hereinafter "CYBER RISK"].

seeking cybersecurity insurance policies are subject to qualitative assessments of their risk management procedures and risk culture as determined by the insurance underwriters.[24]

There are a number of factors that impact the scope and cost of a cyber liability policy, including the size and type of business, the number of customers, the type of data and information the business stores, and the business' online exposure.[25] These individualized policy assessments drive up the cost of cyber insurance policies.[26] Additionally, small businesses will face challenges in obtaining a cyber policy because many small businesses are underequipped to implement adequate risk-management techniques to protect their networks; the ways in which employees access data systems and the reliability of the business' antivirus and anti-malware software will be highly scrutinized when they apply for coverage.[27]

Another major hurdle for small business cyber insurance consumers is the complexity and variability in potential insurance options.[28] In a Council of Insurance Agents and Brokers survey, 55 percent of brokers said cyber insurance coverage was too unclear.[29] The National Association of Insurance Commissioners and the Center for Insurance Policy and Research have outlined different liabilities that may be covered by a cyber insurance policy, including:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expenses related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.[30]

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Sam Friedman and Adam Thomas, *Demystifying cyber insurance coverage, Clearing obstacles in a problematic but promising growth market*, DELOITTE UNIVERSITY PRESS, Feb. 2017, *available at* https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html.
[29] *Id.*
[30] CYBER RISK, *supra* note 21.

IV. Other Challenges for the Cybersecurity Insurance Industry

While more small businesses are exploring the possibility of purchasing cyber insurance policies, disputes between policyholders and insurers are inevitable as courts are asked to interpret cyber insurance policy language and cyber-related claims continue to be made by businesses carrying traditional commercial general liability policies that lack cyber insurance exclusions.[31]

As cyber insurance policyholders continue to become victims of sophisticated schemes designed to coerce businesses into authorizing transfers to fraudulent bank accounts, insurance coverage fights will persist under the computer fraud provisions of commercial crime policies.[32] For example, one particularly important dispute is currently being contested by a Seattle-based seafood company that was unwittingly wired funds to an online fraudster.[33]

V. Policy Considerations for the 115th Congress

Although cybersecurity insurance as a standalone line of coverage offers protection against a wide range of cyber incident losses, few cybersecurity insurance policies provide businesses with coverage for an area of growing private and public concern: the physical damage and bodily harm that could result from a successful cyber attack against critical infrastructure.[34]

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).[35] In addition to the NIPP, other divisions within DHS, particularly the Office of Cybersecurity and Communications[36] and the United States Computer Emergency Readiness Team,[37] 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.[38] The order established DHS as having a lead role in cybersecurity[39] and encouraged the federal government to increase their information sharing with the private-sector entities.[40] The order also directed NIST to develop a

---

[31] Jeff Sistrunk, *4 Key Cybersecurity Insurance Cases to Watch*, LAW360, (July 14, 2017), https://www.law360.com/articles/934228/4-key-cybersecurity-insurance-cases-to-watch.
[32] *Id.*
[33] Aqua Star (USA) Corp. v. Travelers Casualty and Surety, No. 16-35614 (U.S. Court of Appeals, 9th Cir. filed August 1, 2016).
[34] DHS CYBER, *supra* note 20.
[35] DEPT. OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 5-6, *available at* https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. The 2013 plan is based off of the version from 2009. *Id.* at 3.
[36] DEPT. OF HOMELAND SEC., *National Protection and Programs Directorate*, http://www.dhs.gov/xabout/structure/editorial_0794.shtm (last visited Jul. 24, 2017).
[37] US COMP. EMERGENCY READINESS TEAM., *About Us*, http://www.us-cert.gov/about-us.
[38] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[39] *Id.* at § 4, 78 Fed. Reg. at 11,739.
[40] *Id.* at § 4(e), 78 Fed. Reg. at 11,740.

framework to reduce cyber risks to the critical infrastructure.[41] 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."[42] 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.[43]

The Department of Homeland Security's National Protection and Programs Directorate (NPPD) is working with various stakeholders including academia, infrastructure owners and operators, insurers, chief information security officers (CISOs), risk managers, and others to find ways to expand the cybersecurity insurance market's ability to address this emerging cyber risk area.[44] The 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 the help stakeholders offer cybersecurity insurance policies that would incentivize businesses for adopting those best practices.[45]

In March 2016, the NPPD sought input from these various stakeholders on the 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.[46] 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.[47]

In May 2017, President Donald Trump signed a cybersecurity executive order[48] which directs the federal government to responsibly secure it's IT and data and states that agencies must manage their cybersecurity risk according to NIST's Framework for Improving Critical Infrastructure Cybersecurity.[49] Industry experts expect the Trump Administration's prerogative to have a wide-reaching influence on policyholders and insurers. 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

---

[41] *Id*. at § 7, 78 Fed. Reg. at 11,740-41.
[42] *Id*.
[43] 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.
[44] DHS CYBER, *supra* note 20.
[45] *Id*.
[46] 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).
[47] 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.
[48] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May. 11, 2017).
[49] *Id*.

security framework proposed by the NIST"[50] and that "increased compliance with NIST will make the framework even more influential in businesses in all sectors of the economy."[51]

VI. Conclusion

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 that do not have the resources to effectively combat cyber attacks. One possible solution is cybersecurity insurance. Cybersecurity insurance can mitigate losses from cyber incidents, including data breaches, business interruption, and network damage that might otherwise destroy a small business. However, the cyber insurance marketplace is relatively new and faces significant challenges to becoming a singular and comprehensive solution to cyber attacks against small businesses.

[50] *Cyber security framework marches forward,* BUSINESS INSURANCE (Jul. 3, 2017), http://www.businessinsurance.com/article/00010101/NEWS06/912314233/Cyber-security-framework-marches-forward.
[51] *Id.*