ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Daniel Castro

Vice President

Information Technology and Innovation Foundation (ITIF)

Before the

Senate Committee on Small Business and Entrepreneurship

"Preparing Small Business for Cybersecurity Success"

April 25, 2018

428A Russell Senate Office Building

Washington, DC

INTRODUCTION

Chairman Risch, Ranking Member Cardin and members of the committee, my name is Daniel Castro, and I am vice president of the Information Technology and Innovation Foundation (ITIF), a non-profit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity, and director of ITIF's Center for Data Innovation. I appreciate the opportunity to appear before you to discuss opportunities to support small businesses as they seek to improve their cybersecurity practices.

CYBERSECURITY THREATS FACED BY SMALL BUSINESSES

Small businesses face significant cybersecurity threats: In 2015, the National Small Business Association reported that 42 percent of small businesses were victims of cyberattacks.[1] It also found that, on average, cyberattacks cost small businesses approximately $7,000, and when their bank accounts were hacked, their average losses were approximately $32,000.[2] While small businesses generally face the same types of threats as larger businesses, small businesses experience a greater proportion of certain types of cyber incidents, such as malware and phishing attacks.[3] In addition, 58 percent of the confirmed data breaches in 2017 involved small businesses.[4]

Most small businesses are concerned about cybersecurity, but they are not doing enough to protect themselves against cybersecurity threats. One survey by CSID, a security firm owned by Experian, found that while a majority (58 percent) of small businesses are concerned about cyber threats, one-third were "not taking any pro-active steps to protect against cyber threats," and half "do not allocate any budget for risk mitigation services."[5] One reason for this lack of action is that many small businesses underestimate the potential risk they face from cyberattacks. For example, in one survey, 57 percent of small businesses who had not suffered a cyberattack reported that they believed they could recover from a cyberattack within one month. Yet 60 percent of small businesses who had suffered a cyberattack reported that it took them more than a month to recover.[6]

These cybersecurity risks present an existential threat to some small businesses as firms can go bankrupt from the cost of responding to a cybersecurity incident or from the lost revenue and customers resulting from a business disruption caused by a cybersecurity incident. Indeed, the per user cost of these attacks is greater for smaller organizations. In a recent study, Accenture compared the average cost for cybercrime per worker among organizations in the first and last quartile by number of employees. The study found that the average cost among the 25 percent of organizations with the fewest employees was four times as much as the average cost among the 25 percent of organizations with the most employees.[7] In addition, the Better Business Bureau found that more than half of small businesses would be unprofitable within a month if they were to lose permanent access to their essential data—such as would occur after a ransomware attack or hardware failure without data backup.[8]

OPPORTUNITIES TO ENHANCE CYBERSECURITY IN SMALL BUSINESSES

Cybersecurity threats present a major challenge for businesses. While both large and small companies face cybersecurity challenges, larger organizations are generally better equipped to handle cybersecurity threats than smaller ones. Indeed, few small businesses are taking the basic steps necessary to protect themselves from cybersecurity threats. One recent survey found that only 12 percent of small businesses reported having

developed a cybersecurity response plan and only 21 percent reported providing security awareness training to employees.[9]

These cybersecurity vulnerabilities are a drain on the U.S. economy. According to the Council of Economic Advisors, cyberattacks cost the U.S. economy between $57 billion and $109 billion in 2016.[10] Therefore, Congress should take steps to bring small business cybersecurity practices up to par with larger organizations.

These steps should include:

1. Establishing a certification program for "part-time" cybersecurity professionals
2. Creating a cybersecurity boot camp for small businesses
3. Forming a small business cybersecurity co-op

Establish a Certification Program for "Part-Time" Cybersecurity Professionals

One problem small businesses face is difficulty hiring workers with the necessary cybersecurity skills and experience. This problem affects businesses of all sizes. By 2022, the International Information System Security Certification Consortium estimates that there will be a global shortage of 1.8 million cybersecurity workers.[11] In the United States alone, 40,000 cybersecurity jobs go unfilled every year.[12] The cybersecurity workforce shortage is likely to impact small businesses disproportionately, since small businesses tend to pay workers less than larger businesses and thus may have a harder time recruiting workers with highly sought-after cybersecurity skills.[13]

Moreover, in many cases it is impractical for small businesses to hire a dedicated, full-time cybersecurity professional, and so they instead assign these responsibilities to an employee without the proper training who works on these issues on a "part time" basis. Sometimes small business owners are themselves the individuals primarily responsible for managing cybersecurity threats, yet they are unfamiliar with the main cybersecurity risks facing their businesses. In one survey of owners, executives, and senior managers in small businesses, one-quarter had not heard of phishing attacks, one-third had not heard of ransomware, and almost half had not heard about point-of-sale malware that steals credit card data from customers.[14]

Organizations that lack employees with cybersecurity skills contribute to businesses failing to implement many important cybersecurity capabilities, such as multifactor authentication, network and endpoint forensics, and intrusion prevention systems.[15]

One way to address this skills gap is to provide better cybersecurity training to employees in small businesses. Existing efforts appear to be insufficient. For example, the U.S. Small Business Administration (SBA) offers only one cybersecurity training module through its online learning program. This 30-minute class offers participants a basic introduction to cybersecurity issues. However, most of the content is rudimentary to the point of being inconsequential. Moreover, some of the advice in the module is simply impractical, such as "Don't click on links in an email" and "Don't reply to unsolicited emails."[16] The module also does not cover recent cybersecurity threats, such as ransomware. Ironically, users can only access the training module if they install Adobe Flash, a multimedia platform for web content that has been removed or disabled from current versions of most Internet browsers.[17] To view the training content, users must click a link to install Flash on

their computers, violating one of the module's key directives: "Do not allow any websites to install software on your computer."[18]

Other training programs offered for small businesses similarly often lack a high level of rigor because they do not adhere to any standard. While there are many certifications available for cybersecurity professionals, the vast majority of these certification programs are tailored towards dedicated, full-time cybersecurity workers. As such, obtaining these credentials requires more of an investment in time and money than is necessary or practical for small business employees who are only working on cybersecurity issues as a small part of their job. To address this problem, SBA should work with existing professional certification organizations and the private sector to develop a low-cost, vendor-neutral certification program for small business employees who act as their company's designated cybersecurity expert. A panel of cybersecurity experts should regularly review the curriculum to ensure that it is accurate, comprehensive, and up-to-date. SBA could authorize any qualified professional certification organization, such as SANS, ISACA, ISC2, and CompTIA, that accurately assesses mastery of the curriculum to provide the certification. Such a certification would allow small businesses to assess whether they have someone qualified to handle cybersecurity issues and acquire necessary training. It would also ensure that they would not necessarily forfeit workers by overtraining them on cybersecurity skills, which may make them leave their existing job.

SBA should develop open educational materials for those who wish to complete the certification and make these training materials available directly to small business employees online. In addition, these resources could be integrated into in-person training offered by Small Business Development Centers or SBA-affiliated non-profits like SCORE, which provide assistance and mentoring to small businesses.

Create a Cybersecurity Boot Camp for Small Businesses

Some small businesses may never have a trained cybersecurity professional, but they still need instructions on the steps necessary to properly mitigate common cybersecurity threats. To better guide small businesses through the process of creating a basic cybersecurity program, SBA should develop a free online "Cybersecurity Boot Camp" for small businesses that provides participants the concrete steps they need to develop to identify, protect, detect, respond, and recover from cybersecurity incidents. The goal of the boot camp would be to raise the baseline level of security for any participant to address the most critical cyber threats facing small businesses. Participants would not be expected to come with any prior knowledge and they could repeat the boot camp as often as necessary. SBA should be required to update the curriculum regularly, so that it is contains information on known as well as emerging threats.

Virtually none of the existing resources the federal government makes available for small businesses offers this type of concrete, step-by-step guidance on how to implement the most effective cybersecurity tactics. Instead, most of the government-provided resources either describe basic objectives (e.g. "use strong passwords") or describe cybersecurity issues (e.g. defining terms like "distributed denial of service attack"). Small businesses need much more practical guidance. To understand why the federal government's current approach is ineffective, imagine if stores like Ikea provided their customers one-pagers explaining the importance of not over-tightening screws and pamphlets on the dangers of collapsing bookshelves, instead of step-by-step instructions on how to assemble furniture. Small businesses, especially those lacking IT professionals, need the detailed instructions.

Small businesses have limited resources to address cybersecurity threats, so the SBA should better curate the information presented to small businesses about how to address cybersecurity threats on its own site as well as that of its partners. While many different government agencies offer resources about cybersecurity for small businesses, they do not explain or describe how each resource differs from the others, contributing to information overload for small businesses. In addition to what the SBA provides directly and in partnership with the National Cyber Security Alliance, agencies such as the Department of Homeland Security, the National Institute of Standards and Technology (NIST), the Federal Communications Commission (FCC), and the Federal Trade Commission (FTC) all offer their own cybersecurity resources to small businesses.

Moreover, many of these sites are not user friendly, containing broken links or requiring users to navigate through multiple pages to find to the content. For example, one link on the FCC's website to its primary guide for small businesses leads to an error page with the message, "Your request looked malicious and has been blocked."[19] In addition, many resources, such as the FCC's one-page handout "Ten Cybersecurity Tips for Small Businesses," are undated and others, such as the FCC's Small Biz Cyber Planner 2.0, are outdated.[20] Government provided cybersecurity resources should be current, and agencies should be directed to withdraw or replace older materials to ensure small businesses are accessing accurate information.

SBA should promote its cybersecurity resources with all partners, including other federal and state programs as well as private sector initiatives, that work with small business, such as NIST's Manufacturing Extension Partnership Program, the Department of Commerce's Minority Business Development Agency, and the U.S. Chamber of Commerce.

Form a Small Business Cybersecurity Co-Op

One challenge small businesses face is that some cybersecurity products and services have high per-user costs when they purchase services for a relatively small number of employees. Often vendors offer variable pricing based on the number of users or require a minimum purchase amount. These high per-user costs make these solutions unattractive or unfeasible for many small businesses. One reason vendors charge more on a per-user basis for smaller companies is because they have fixed customer acquisition costs.

For example, consider how businesses attempt to mitigate the threat of phishing attacks. Phishing attacks are a social engineering attack wherein an attacker attempts to impersonate a trusted entity, such as a financial institution or work colleague, to steal information from a potential victim by sending a message containing a malicious link or attachment that the unsuspecting target then opens. Between October 2013 and December 2016, the FBI's Internet Crime Complaint Center (IC3) tracked approximately 22,000 phishing attacks affecting U.S. businesses resulting in nearly $1.6 billion in losses, mostly from fraudulent bank transfers.[21] And a survey of small businesses found that 20 percent report having been victims of a phishing attack.[22]

Stopping these attacks is exceedingly difficult because the exact nature of the message changes frequently. Many businesses have found that one of the most effective ways to prevent these attacks is by conducting phishing simulations. Phishing simulations involve sending innocuous phishing attempts to employees using the same techniques employed by attackers. If employees fall for the rouse, rather than infecting their machine, they are given the opportunity to complete additional security awareness training. Unfortunately,

cybersecurity vendors providing this type of phishing simulation service do not cater to small businesses, even though these businesses receive a disproportionate number of these types of attacks.[23]

SBA could assist small businesses by establishing a cybersecurity cooperative to create a large pool of willing buyers for various cybersecurity products and services, including cyber risk insurance. Participation in the Cybersecurity Co-Op could be open to any small business, and depending on the level of interest, could be organized around particular regions or sectors. The co-op could identify and evaluate cybersecurity products and services for its members and negotiate better rates for its users than they could get on their own. This would allow small businesses to get more value for their investments in cybersecurity and increase adoption of best-in-class cybersecurity tools.

CONCLUSION

Small businesses face many cybersecurity threats, and there is more the federal government can and should do to help small businesses succeed in addressing these threats. In addition to the recommendations outlined above, this committee, through its oversight, can insist that SBA provide small businesses timely and effective training materials about mitigating cybersecurity threats. However, these steps can ultimately fix only part of the problem. The greater challenge for the U.S. government is to reform its national cybersecurity policy to move away from an emphasis on relative offensive capabilities and instead prioritize absolute defensive capabilities, including prosecuting cybercrime. Such a change would require substantially rethinking how the U.S. government allocates funding for cybersecurity, how it releases cybersecurity research into the public domain, and how it works cooperatively with the private sector, through a reformed vulnerabilities equities process (for zero-day exploits) and expanded bug bounty programs.

REFERENCES

1. "2015 Year End Economic Report," National Small Business Association, 2016, http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
2. "2015 Year End Economic Report," National Small Business Association, 2016, http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
3. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.
4. "2018 Data Breach Investigations Report," Verizon, 2018, https://www.verizonenterprise.com/verizon-insights-lab/dbir/.
5. "Survey: Small Business Security," CSID, May 2016, https://www.csid.com/wp-content/uploads/2017/01/WP_SmallBizSecurity_2016.pdf.
6. "National Survey Reveals Most Small Businesses Unprepared for Cyber Attacks," Nationwide, 2016, https://www.nationwide.com/about-us/101316-cybersecurity.jsp.
7. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.
8. "2017 State of Cybersecurity Among Small Businesses in North America," Better Business Bureau, 2017, https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.
9. "Survey: Small Business Security," CSID, May 2016, https://www.csid.com/wp-content/uploads/2017/01/WP_SmallBizSecurity_2016.pdf.
10. "The Cost of Malicious Cyber Activity to the U.S. Economy," Council of Economic Advisors, February 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.
11. "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," ISC(2), June 7, 2017, https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage.
12. Jeff Kauflin, "The Fast-Growing Job With A Huge Skills Gap: Cyber Security," Forbes, March 16, 2017, https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/.
13. Anthony Caruso, "Statistics of U.S. Businesses, Employment and Payroll Summary: 2012," February 2015, U.S. Census Bureau, https://www.census.gov/content/dam/Census/library/publications/2015/econ/g12-susb.pdf.
14. "2017 State of Cybersecurity Among Small Businesses in North America," Better Business Bureau, 2017, https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf.
15. "Cisco 2018 Annual Cybersecurity Report," Cisco, 2018, https://www.cisco.com/c/en/us/products/security/security-reports.html.
16. "Cybersecurity for Small Businesses," U.S. Small Business Administration, n.d., https://www.sba.gov/course/cybersecurity-small-businesses/ (accessed April 20, 2018).

17. Gregg Keizer, "FAQ: How Apple, Google, Microsoft and Mozilla will eliminate Adobe Flash," ComputerWorld, July 31, 2017, https://www.computerworld.com/article/3211437/web-browsers/faq-how-apple-google-microsoft-and-mozilla-will-eliminate-adobe-flash.html.

18. "Cybersecurity for Small Businesses," U.S. Small Business Administration, n.d., https://www.sba.gov/course/cybersecurity-small-businesses/ (accessed April 20, 2018).

19. See link to https://www.fcc.gov/cyber/cyberplanner.pdf on page https://www.fcc.gov/cyberplanner (access April 22, 2018).

20. The FCC created the Small Biz Cyber Planner 2.0 in 2012.

21. "Business Email Compromise, Email Account Compromise, The 5 Billion Dollar Scam," Public Service Announcement, Federal Bureau of Investigation, May 4, 2017, https://www.ic3.gov/media/2017/170504.aspx.

22. "National Survey Reveals Most Small Businesses Unprepared for Cyber Attacks," Nationwide, 2016, https://www.nationwide.com/about-us/101316-cybersecurity.jsp.

23. "2017 Cost of Cybercrime," Accenture, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf.