CompTIA

United States Senate Committee on Small Business and Entrepreneurship

"Cyber Crime: An Existential Threat to Small Business"

Testimony by Elizabeth Hyman, Executive Vice President, CompTIA
March 13, 2019

Introduction

Chairman Rubio and Ranking Member Cardin, on behalf of the Computing Technology Industry Association (CompTIA), thank you for having me here today. CompTIA is the leading voice and advocate for the $1.6 trillion US global information technology ecosystem, and the more than 11.5 million American information technology (IT) professionals who design, implement, manage, and safeguard the technology that powers the world's economy.[1] Through education, training, certifications, advocacy, philanthropy, market research and membership programs, CompTIA is the hub for advancing the tech industry and its workforce.

As you well know, small business is the backbone of our economy. However, our small businesses are at risk from hackers and nation states. Small businesses have fewer employees and resources than large enterprises and are fertile targets for cyber criminals looking to exploit vulnerable defenses. Our nation's small businesses need help.

CompTIA works with small business members and countless small business customers on a daily basis and we are committed to working with this committee to ensure that all business owners are educated on and protected from the threats they are facing.

Sizing Up Today's Threats

At one time, cyberattacks were just an "IT problem" that featured such nuisances as defaced websites, occasional viruses that made the lives of IT workers miserable, or the odd hacked e-mail account or two. Sometimes, individuals heard about cybersecurity problems when their credit card was compromised. Occasionally, an astute individual may have heard of a Distributed Denial of Service (DDoS) attack or news about a few obscure wily hackers who had stolen someone's identity. Traditional security approaches had the ability to manage many of these attacks.

Conditions have changed dramatically over the last five years. Our society is becoming more connected and the proliferation of IoT and other systems will only increase this trend. As CompTIA research suggests, cybersecurity issues have grown in size and scope, becoming more sophisticated, harder to detect and more widespread (see attached report on The Evolution of Security Skills). They have also increasingly been aimed at the pillars of our society: credit agencies, major retailers, government and military departments, information services and elements that underpin our democratic processes are under regular attack.

[1] www.comptia.org

To compound the threat, regular users and IT professionals alike do not always have adequate skills to protect themselves and others. In 2017, we saw the proliferation of successful "phishing" attacks that trick individuals into revealing sensitive information (e.g. passwords) or installing malware on their system[2]. In February of 2018, a company called GitHub experienced the largest DDoS attack ever recorded.[3]

It is worth noting that according to the 2018 Verizon Data Breach Investigation Report, 58% of breach victims were characterized as small businesses.[4] We have seen the trend of cyber attackers shifting their attack patterns to exploit third- and fourth-party supply chain partner environments to gain entry to target systems.[5] We need only look as far as the massive Target breach of 2013, where it is believed that hackers gained access to the Target network by successfully hacking a small business vendor to the retail giant, to appreciate the idea that we are all vulnerable to the weakest link in our digitally connected economy.[6]

The overall costs of cybersecurity compromises are enormous. Research by Cybersecurity Ventures estimates that by 2021, cybercrimes will cost $6 trillion per year worldwide.[7] This includes not only stolen money and ransom, but also the value of lost productivity and intellectual property, data theft, business disruption, reputational harm and more. As a result, many organizations are finding it difficult to keep up with the costs of protecting data and sensitive information.

The Cybersecurity Challenges for Small Businesses

Traditionally, small businesses have invested less in cybersecurity because of limited resources or the assumption that their digital assets are of less value to cybercriminals. With any form of digital data now holding some value (customer data, employee information, records relating to government clients, etc.), businesses of all sizes must view cybersecurity as a vital business expense. According to CompTIA research, only 14% of businesses with less than 100 employees feel that their current cybersecurity strategy is completely satisfactory, compared to 20% of businesses with 100-499 employees and 27% of businesses with 500 or more employees.[8] While

---

[2] APWG *Phishing Activity Trends Report, First Half 2017*, October 2017, http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf

[3] Wired Magazine, *GitHub survived the biggest DDoS attack ever recorded*, March 1, 2018, https://www.wired.com/story/github-ddos-memcached/

[4] *Verizon Data Breach Investigation Report, 2018*, https://enterprise.verizon.com/resources/reports/dbir/

[5] Accenture, "*Ninth Annual Cost of Cybercrime Study*," March 6, 2019, https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[6] CNBC, "*Congress addresses cyberwar on small business: 14 million hacked over last 12 months*," April 5, 2017 https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html

[7] Cybersecurity Ventures, *2017 Cyber Crime Report,* October 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[8] CompTIA *2018 Trends in Cybersecurity: Building Effective Security Teams*, September 2018, https://www.comptia.org/resources/cybersecurity-trends-research

improved cybersecurity is needed across the board, small companies are the ones with the steepest challenge. CompTIA research shows that only 62% of small businesses have internal resources focused on security, compared to 91% of mid-sized businesses and 95% of large firms.[9]

The first part of the challenge is awareness of the scope of modern cybersecurity. Along with understanding that all digital assets are valuable, small businesses must understand the risk of a cybersecurity breach. According to the *2018 Cost of a Data Breach Study* by IBM/Ponemon, the average cost of a data breach to a company is $3.86 million or $148 per stolen record.[10] Although a small business may have fewer records impacted in a breach, the cumulative sum is more likely to have a catastrophic impact due to lower operating margins.

The variety of attacks has grown dramatically with the adoption of new technology models, and small businesses have low awareness of the many attack formats. For example, 64% of small firms believe that a virus could affect their business, but only 33% believe that ransomware could be a factor and 19% are concerned about a DDoS attack.[11] These other attacks take a very different form and require different forms of defense.

How the Small Business Administration Can Help Advance a Three-Pronged Defense

Small Business Development Centers (SBDCs) managed by the SBA can play an important role in helping to address the challenges unique to the cybersecurity of small businesses. To properly assist small businesses, the SBDCs should focus on improving the three key elements of modern security:

1) Technology tools
2) Business processes
3) Effective employee education

A. Improved Technology Tools: Understanding the Tools Needed

From a technology perspective, many companies have previously focused on a limited set of defensive tools (primarily firewall and antivirus). A modern security toolset expands to include protections that fits current usage, such as Data Loss Prevention (DLP), Identity and Access Management (IAM), and Security Information and Event Management (SIEM). There are also more proactive tools and methods being used, such as penetration testing that proactively assesses the strength of the overall defenses. At a minimum, cybersecurity experts advising small businesses should be familiar with the full suite of security tools available today.

---

[9] CompTIA Research Report, *2018 Trends in Cybersecurity: Building Effective Security Teams*, September 2018, https://www.comptia.org/resources/cybersecurity-trends-research

[10] IBM, *2018 Cost of a Data Breach Study: Global Overview* (by Ponemon), July 2018, https://www.ibm.com/security/data-breach

[11] CompTIA Research Report, *The Evolution of Security Skills*, April 2017, https://www.comptia.org/resources/the-evolution-of-security-skills

B. Business Processes: Measuring for Success

Building secure processes is a separate step that touches all corners of a business. Processes range from developing an incident response plan to taking simple steps to educate and test employees on basic cyber hygiene. There are many existing government resources to assist SMBs in this exercise. For example, cybersecurity advisors (also known as CSAs) are regionally-located DHS personnel who offer immediate and sustained cybersecurity assistance to prepare and protect organizations, including small and mid-sized businesses.[12] CSAs should be focused on helping small businesses understand how to build security policies and establish proper enforcement. This will include internal operations as well as relationships with outside suppliers or partners.

Regardless of the public partner, it may behoove the SBDC to consider bestowing an organizational designation similar to CompTIA's Security Trustmark (which is based on the NIST critical infrastructure cybersecurity framework) upon completion of some sort of evaluation. This designation would help the small business demonstrate to clients that they are well versed on modern cybersecurity issues and have the processes and personnel equipped to perform digital business in a secure fashion.

In addition, small businesses should have the ability to learn from each other. As has been raised in previous congressional sessions, the idea of sharing threat information between small businesses and the government is one that could add significant value to our cyber defenses.[13] Taking it one step further, the sharing of best practices on an SBA-managed platform that is populated by businesses self-reporting (perhaps in an anonymous but verified way) could prove to be an invaluable and low-cost resource for small businesses. Seeing how other similarly situated organizations have both increased their cybersecurity and responded to incidents would no doubt help to alleviate concerns for new businesses who are just getting started or existing ones facing a breach.

Ultimately, however, small businesses will need metrics to track the effectiveness of their security programs and processes. Metrics should be derived from real experience, based on private and public sector best practices and through careful coordination. It doesn't take as much time to do this as individuals might think -- real-time measurements can be created after an hour or two of coordination. If cybersecurity professionals and business leadership properly translate technical specifications and business objectives into proper communication, then organizations will have gone a long way to solving long-standing problems. Sample metrics can include improving employee/end-user education by instituting phishing and other simulations and tracking results, lowering containment times (e.g., the time between a security breach and its resolution), and response times (e.g., the amount of time it takes to restore a critical business service).

[12] https://www.sba.gov/managing-business/cybersecurity/top-tools-and-resources-small-business-owners

[13] H.R. 4668, Small Business Advanced Cybersecurity Enhancements Act of 2017; H.R. 3002, Small Business Cyber Training Act of 2017

C. Effective Employee Education: Leveraging Vendor Neutral Industry-Recognized Credentials

There is a shortage of cybersecurity workers in the United States.[14] Though a national shortage is of significance to businesses of all sizes, small businesses are at a particular disadvantage when it comes to recruiting talent. Salary sensitivity is greater when there is a demand for skilled labor. Still, there are very practical and affordable steps that SMBs can take to build expertise in all the areas that are needed for modern cybersecurity. It is especially vital to ensure that a small business IT team, which fulfill many roles, has a solid foundation in security skills, sufficient specialized expertise in a few key areas, and then the ability to work with an outside partner, such as a managed security services provider, when deep expertise is called for.

CompTIA is one of several vendor neutral certifying bodies that offer certifications that are ANSI and ISO accredited. Nevertheless, to provide greater context for this submission, we offer a description of the many tools that CompTIA presently offers.

CompTIA's Security Pathway includes certifications that describe the basics of IT systems (such as ITF+ and A+), certifications that describe the technical aspects of cybersecurity (such as Security+, CySA+, and PenTest+), and the CASP+ certification that describes the implementation of cybersecurity solutions based on organizational policies.

IT Fundamentals (ITF+) is a vendor-neutral certification that covers a broad range of knowledge and skills required of employees who have to operate within an enterprise driven by technology. Professionals operating in small- to mid-size companies many times have to bear the burden of wearing multiple hats, requiring them to have a broader range of IT skill sets. ITF+ covers topics such as IT Concepts and Terminology, Infrastructure, Application and Software, Software Development basics, Database fundamentals and cyber security. This program will ensure non-IT staff (or new IT staff) have a broad range of knowledge related to technologies and security concepts that impact them on a daily basis.

For IT support staff and other IT personnel, CompTIA's A+ and Security+ certifications are the perfect combination to ensure these staff members are well versed with the skills and abilities required to successfully perform on the job.

The A+ vendor-neutral certification covers the full gamut of knowledge and skills required to support all common hardware, devices, technologies and operating systems used in small and large corporate environments. In addition, the certification also addresses skills needed to manage basic networks, implement techniques to secure all common types of client-side devices (IoT) and understand how to best leverage cloud and virtualization technologies.

CompTIA's Security+ certification is targeted at general IT support staff who have been operating within an IT environment for approximately 2 years with a focus on security. This

[14] https://www.cyberseek.org/

certification takes a deeper dive into the challenges of securing corporate infrastructure. Professionals will need to prove competency in the areas of threats, attacks and vulnerabilities, technologies and tools used to remedy security concerns, best practices for architecture and design, identity and access management, risk management, and the importance of cryptography and public key infrastructure (also known as PKI, it is used to efficiently ensure encrypted communications can take place).

Candidates who complete the proposed pathway of all three of these certifications will have the requisite knowledge and skills to provide a broad range of IT support across many diverse platforms in small business environments while maintaining an aggressive security posture against all types of corporate threats.[15] In addition, many employers may not know what to look for when seeking out cybersecurity and IT personnel. By knowing to look for personnel that have vendor-neutral certifications, it will help to not only validate skills, but also enable employers to cross reference the skills they need with those that a certification exam is testing on.

Policy Considerations: Federal Data Breach and Notification Law

While this hearing is focused on practical steps to aid small businesses in their cybersecurity readiness, we would be remiss if we did not point out one policy consideration that we believe would be of great assistance to small businesses. Data breaches have become part of the cost of doing business. With the increasingly mobile and decentralized nature of our economy and data storage and dissemination technologies, most companies are under the umbrella of multiple state laws at all times. The need to comply with as many as 50 different state data breach notification laws is one of the drivers of the high-costs associated with data breaches. While larger organizations may be able to foot this bill and still remain in business without breaking a sweat, these are numbers that could quickly bankrupt many small businesses.

We encourage Congress to work with industry to develop a single federal standard for data breach notification. This will help alleviate these burdensome compliance costs and instead allow for SMBs to devote their time and resources to investigating and resolving the breach. The ability to do so will also better protect the consumers whose information was stolen.

Incorporate a Culture of Cybersecurity to Businesses of All Sizes

Finally, it is vital that we focus on establishing a culture of cybersecurity within any organization to help not only defend against attacks, but also help with the aftermath of an attack or breach. As CompTIA outlined in our white paper entitled, "*Building a Culture of Cybersecurity: A Guide for Executives and Board Members,*"[16] there are 6 principles that all organizations can adopt on a scale that is appropriate to their business:

- **Integrate cybersecurity into business strategy**: Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business

[15] Those candidates wishing to progress along a cybersecurity career path can proceed to the more advanced exams of CySA+, PenTest+, and the CASP+ certification that describes the implementation of cybersecurity solutions based on organizational policies.

[16] CompTIA White Paper, *Building A Culture of Cybersecurity: A Guide for Executives and Board Members*, April 2018, https://www.comptia.org/resources/building-a-culture-of-cybersecurity-a-guide-for-corporate-executives-and-board-members

and lead the way in advancing new approaches to cybersecurity costs—and returns.

- **Corporate structure should reinforce a culture of cybersecurity**: If cybersecurity is not built explicitly into an organization, leadership is sending a message that it is not truly committed to the goal.

- **Employees are the biggest risks**: Employees may inadvertently jeopardize data, steal information for a competitor, or sell data or intelligence. Controlling access to company data can significantly improve the chances of catching this behavior before it causes devastating damage.

- **Detect, detect, detect**: The longer it takes to detect a data breach, the more expensive the data breach becomes.

- **Data protection**: Collect what is needed, share only what has to be shared. Organization needs to have flexible and adaptable approaches to protect data.

- **Develop robust contingency plans (and test them!)**: Companies must create a formal incident response team to have an end-to-end cybersecurity strategy.

SBDCs can and must play a role in imparting these principles to small businesses. We must work together as industry and government to lead by example so that company culture can truly embrace cybersecurity. SMBs must view cybersecurity as part of the broader risk management process for their business, rather than jettisoning it off as just a technology problem with a technology solution.

Conclusion

While the challenge that lies ahead of us can seem overwhelming and almost too great a burden to bear, it is one we cannot afford to ignore. By working together and continuing to embrace the private-public partnership that has long benefited the cybersecurity ecosystem, we can do a great deal to help better prepare small businesses, and business of all sizes, for the cybersecurity threats they are facing. Thank you for the opportunity to participate in this hearing and we look forward to further engagement with your Committee.

Respectfully,

Elizabeth Hyman

Executive Vice President, Public Advocacy