NYDIA M. VELAZQUEZ, NEW YORK
CHAIRWOMAN

BLAINE LUETKEMEYER, MISSOURI
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:	Nydia M. Velázquez, Chairwoman
DATE:	July 20, 2021
RE:	Full Committee Hybrid Hearing: "Strengthening the Cybersecurity Posture of America's Small Business Community"

The Committee on Small Business will meet for a hybrid hearing titled "Strengthening the Cybersecurity Posture of America's Small Business Community." **The hearing is scheduled to begin at 10:00 A.M. on July 20, 2021, in person in 2360 Rayburn House Office Building, and virtually via the Zoom platform.**

Small businesses are highly vulnerable to cybersecurity threats as employers, suppliers, and consumers in a modern digital economy. Many cannot afford dedicated Information Technology (IT) staff to navigate and mitigate risks and are wary of investments in pricey software. This hearing will provide members the opportunity to examine the many cybersecurity threats facing small businesses and identify available resources.

Panel

- Ms. Tasha Cornish, Executive Director, Cybersecurity Association of Maryland, Baltimore, MD
- Ms. Sharon Nichols, State Director, Mississippi SBDC, University, MS
- Ms. Kiersten Todt, Managing Director, Cyber Readiness Institute, New York, NY
- Mr. Graham Dufault, Senior Director for Public Policy, ACT, The App Association, Arlington, VA

Background

Whether it is used for paying employees and suppliers, accounting and tax reporting, or interacting with customers, the internet has been a valuable tool for small businesses; the COVID-19 crisis made technology adoption critical to business survival. In a recent survey, the Connected Commerce Council found that 72 percent of small businesses increased use of digital tools during the COVID-19 crisis, and 48 percent utilized a new digital tool.[1] Of all digital tools, video conferencing (38 percent) and social media (31 percent) had the highest usage increase.[2] As more small businesses adopt digital tools, they become more vulnerable to cybersecurity attacks. These

[1] CONNECTED COMMERCE COUNCIL, *Digitally Driven 2021* 28(Mar. 17, 2021), *available at* https://connectedcouncil.org/wp-content/uploads/2020/09/Digitally-Driven-Report.pdf.
[2] *Id.* at 29.

incidents can have major consequences, but small businesses may not have the resources to mitigate cyber risks.

Small Business Cyber Threats

Small businesses are expected to protect financial data and personally identifiable information of customers, employees, and partners against constantly evolving cyber threats. Businesses must consider and secure various technologies including web and e-mail servers, internal networks, remote access, and backup and storage areas.

Common Types of Cyberattacks

Most cyberattacks are launched to gain or increase access to networks in order to steal, alter, or destroy data and information systems. According to the Government Accountability Office (GAO), these are the most common cyberattacks:[3]

- Business email compromises are sophisticated scams carried out by threat actors compromising email accounts through social engineering (e.g., spoofing of a legitimate known email address) or computer intrusion techniques (e.g., malicious software that can gain access to legitimate email threads about billing/invoices) to conduct unauthorized transfer of funds.
- A data breach is an unauthorized or unintentional exposure, disclosure, or loss of an organization's sensitive information. This information can include personally identifiable information (PII), such as Social Security numbers, or financial information, such as credit card numbers.
- A denial-of-service attack is one that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
- Malware, scareware, and viruses are software or code intended to damage or disable computers and computer systems.
- Ransomware is a type of malware used to deny access to IT systems or data and hold the systems or data hostage until a ransom is paid.

Cyberattack Consequences

According to the National Institute of Standards and Technology (NIST), impacts of information security events on small businesses could include: [4]

- damage to information or information systems.
- regulatory fines and penalties / legal fees.
- decreased productivity.
- loss of information critical in running your business.
- an adverse reputation or loss of trust from customers.
- damage to your credit and inability to get loans from banks.
- loss of business income.

---

[3] U.S. GOV'T. ACCOUNTABILITY OFFICE, "HIGH-RISK SERIES: FEDERAL GOVERNMENT NEEDS TO URGENTLY PURSUE CRITICAL ACTIONS TO ADDRESS MAJOR CYBERSECURITY CHALLENGES" (GAO 21-288), 7(Mar. 24, 2021), *available at* https://www.gao.gov/assets/gao-21-288.pdf.

[4] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T. OF COMMERCE, SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS (NISTIR 7621), 4 (2016), [hereinafter "NISTIR 7621"], *available at* https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

Because small businesses are often part of the supply chain for large companies and government procurement systems, a breach could have significant impact on the larger economy.

Cybersecurity Challenges for Small Businesses

In a digital economy, small businesses must take on greater cyber risks, but mitigation investment has not kept pace. This is due to numerous factors such as a lack of time, skills, or finances to build an effective defense. To protect against both inside[5] and outside attacks,[6] a business must ensure they have multiple layers of security, both technological and human.

High Implementation Costs: Technology Investment

Small businesses are largely unaware of the risks associated with wireless networks and e-commerce. In fact, some small firms do not even become aware of the need for computer security planning, until they are victimized by an attack. Consequently, they typically focus on improving cybersecurity only to the extent necessary to continue their business operations or to comply with regulations. Many don't know what types of cybersecurity products and services would best meet their needs before, during, and after a cyber-attack. These products can have high per-unit costs for small-scale purchases and many products have minimum purchase amounts. High costs and information gaps make these solutions unattractive or unfeasible.

High Implementation Costs: Human Investment

When compared to their larger counterparts, small firms often do not have the resources to hire and retain a dedicated cybersecurity team so the owner or a designated employee must also serve as a part-time IT expert. In addition to daily troubleshooting, this role requires expertise on managing technology vendors. Part-time attention makes it difficult to keep up with technologies and strategies needed to protect the business against rapidly evolving cybersecurity threats.

Federal Cybersecurity System

Federal agencies offer a variety of resources to offset some of the technology and human costs of cybersecurity investment.

NIST Framework

As directed by Executive Order 13636, Improving Critical Infrastructure Cybersecurity,[7] the NIST published Version 1.0 of the Cybersecurity Framework in 2014.[8] The Framework was created as voluntary and customizable guidance for organizations to mitigate cybersecurity risks.[9] There are 3 components:

---

[5] Inside attacks include attacks from service providers who have been granted access to a network or specific business information. These threats also comprise of partner companies or third parties who are used to expand a business, run the website, or administer the IT system.

[6] Outside attacks include a situation where an outside party hacks into a business's IT system or physically steals the equipment.

[7] E.O. 13636- IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb 12, 2013) 78 FR 11737 *available at* https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[8] An updated Framework Version 1.1 was released in 2018.

[9] Small business specific Framework and guidance is available in the SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS, NISTIR 7621 *supra* note 9.

- The Framework Core is organized into five Functions—Identify, Protect, Detect, Respond, Recover, which represent basic cybersecurity activities.[10]
- The four Framework Implementation Tiers represent an increasing degree of rigor and sophistication in cybersecurity risk management practices for organization self-assessment and goal setting.[11]
- Framework Profile enables organizations to establish a roadmap for reducing cybersecurity risk aligned with their unique needs. [12]

NIST hosts the Small Business Cybersecurity Corner which is a one stop shop for free guidance, solutions, and training specific to small business needs.[13]

Cybersecurity & Infrastructure Agency (CISA)

The CISA was established in 2018 to improve the nation's capacity to defend against cyber-attacks, from the government level to individual households. It offers small business specific resources through the STOP.THINK.CONNECT.™ public awareness campaign.[14] Cybersecurity awareness campaigns are often used to help small businesses give their employees basic tools to reduce vulnerability through reminders about safeguarding passwords, avoiding phishing schemes, and securing laptops and other mobile devices. Like NIST, CISA has links to federal small business tools, including the Federal Communications Commission Cyberplanner to help create customized cybersecurity plans.[15]

Conclusion

It is important for small companies to be protected against cybercrimes, particularly because of their role in the national economy. However, many small businesses cannot afford the investments necessary to mitigate cybersecurity risks. Because cybersecurity data is usually compiled through surveys conducted by industry associations and incident reports from technology vendors, there is no holistic measure of cyber-attacks on and their impact on small businesses. Federal agencies and the private sector must continue to collaborate on resources, training, and technical assistance to understand and reduce small businesses cyber vulnerabilities.

[10] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T. OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 6(Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[11] *Id*., at 10.
[12] *Id*., at 11.
[13] https://www.nist.gov/itl/smallbusinesscyber.
[14] https://www.cisa.gov/publication/stopthinkconnect-small-business-resources.
[15] https://www.fcc.gov/cyberplanner.