ACT | The App Association

Testimony of
Morgan W. Reed

Before the
U.S. House of Representatives Small Business Committee
November 15, 2017

Executive Summary

Chairman Chabot, Ranking Member Velázquez, and distinguished members of the Committee: My name is Morgan Reed, and I am the president of ACT | The App Association. I thank you for holding this important hearing on improving cybersecurity for small businesses.

ACT | The App Association represents more than 5,000 app makers and connected device companies across the United States that continue to grow and create American jobs in every congressional district. Alongside the embrace of mobile technology across consumer and enterprise contexts, our members have been creating innovative solutions to improve workplace productivity, accelerate academic achievement, and help people lead healthier lifestyles.

In our current environment, cybersecurity threats can seem incomprehensibly vast and inevitable, especially for small businesses. In 2014, 71 percent of companies admitted they fell victim to a successful cyber-attack.[1] Meanwhile, the amount of data online is expected to increase 50-fold by 2020,[2] signaling accelerated tech innovation but also adding new attack vectors due to increased connectivity and a sweetening of the pot for potential cyber criminals. Cybersecurity risk management strategies must keep pace with this growing threat—a task that evolves as more online traffic and commerce is dedicated to the internet of things (IoT).

We support ongoing and emerging public-private partnership initiatives and strategies to improve the nation's cybersecurity risk management posture. But we believe that the small businesses representing 99.7 percent of U.S. firms[3] require heightened focus and assistance and must play a much more significant role in these strategies. Policymakers must remain mindful of the fact that large companies often have expansive budgets available to create and maintain cybersecurity control processes and have the luxury to hire staff and outside consultants to address cybersecurity risks, but small and medium-sized enterprises (SMEs) do not. For many App Association members, chief security officer may be just one of five hats worn by a single employee. The essential role of American small businesses, along with the unique resource constraints they face, make this Committee's work more important to the security and stability of the nation's economy.

Small and medium-sized tech companies like our members exist to solve problems. Take Canned Spinach for example, an App Association member company based in Chairman Chabot's district. Canned Spinach, led by partner Andrew Savitz, uses cutting-edge security-by-design processes to create custom software solutions that streamline backend processes and enhance business-to-business relationships. The services he provides fill a niche and solve problems, most often helping other small businesses access the opportunity of the app economy in a secure and sustainable way. Canned Spinach's approach is representative of all App Association members' in proactively and responsibly managing cybersecurity risks.

Further, the symbiotic platform-developer relationship drives innovative cybersecurity risk management, providing benefits across consumer and enterprise contexts. For example, the small businesses that use Etsy,[4] headquartered in Ranking Member Velázquez's district, agree to use strong data security methods[5] when they handle consumer data on the platform. In this way, Etsy's contractual terms help drive both dynamic risk management practices and good 'cyber hygiene,' small businesses are not alone when it comes to cybersecurity. Small businesses know the platforms they use to sell their services and goods—whether they be Apple, Microsoft, or Etsy—are there to hold them accountable but also to help them meet their obligations on cybersecurity.

Alongside the development of private sector-driven cybersecurity activities, the federal government should take focused, concrete steps to help SMEs succeed in security. To better protect your constituents and our customers, we need your help in three specific ways: First, we need the federal government to improve its information sharing activities; second, the federal government should take steps to make cybersecurity frameworks and best practices more workable for SMEs; and third, the federal government should ensure a legal and policy environment that enhances SMEs' ability to adequately manage dynamic cybersecurity risks. To this end, I will elaborate on three main points in my testimony:

- The federal government should make the cybersecurity threat information it shares timely, more accessible, and more useful to SMEs.
- The federal government should help SMEs improve their understanding of cybersecurity risk management by developing and widely publicizing targeted, user-friendly, and compelling best practices and guidance that is built on key public-private partnership-driven deliverables such as the National Institute of Standards and Technology's (NIST) voluntary Cybersecurity Framework.[6]
- Congress should take steps to provide legal and policy certainty that SMEs can rely on when they leverage the best technical protection mechanisms (TPMs) available. For example, Congress should pass the International Communications Privacy Act (ICPA, H.R. 3718 and S. 1671) to clarify SMEs' legal liability in data requests, and maintain a legal environment that supports investment in cybersecurity.

Thank you for the opportunity to share insights on behalf of our member companies. I look forward to a productive discussion about how we can encourage better cybersecurity practices by SMEs in your districts.

I. The Federal Government Can Help SMEs Improve Cybersecurity

a. Small Businesses Leverage Security Infrastructure Offered by Large Company Platforms

Fortunately, SMEs are often able leverage the numerous security features and capabilities larger platform and cloud service provider companies offer. In this manner, SMEs can offload security infrastructure overhead. Microsoft's Azure, for example, has worldwide visibility into cyber threats and is able to observe based on what all of its users are reporting to the platform. Azure invests about $1 billion annually to advance its efforts on security, data protection, and risk mitigation, and employs over 3,500 security professionals.[7] These experts take measures such as setting up honeypots to attract cybercriminals and watch how they behave—intelligence that SME users of Azure benefit from directly. Beyond cloud services, Apple HealthKit provides a platform that defends against cyber threats on behalf of the SMEs who build products on top of it. And Intel has created a new Sawtooth chip to enable enterprise blockchain frameworks on which SMEs can innovate in a secure fashion. These various platform-SME relationships point to the many ways SMEs can leverage security infrastructure offered by the platforms. However, these arrangements do not tell the whole story and there remains significant work the federal government can do to improve information sharing for SMEs.

b. Awareness and Enhancement of Information Sharing Efforts

The Department of Homeland Security (DHS) has undertaken several efforts to facilitate timely cyber threat data sharing over the years. Unfortunately, the structure and mechanics of information sharing are complicated. The main private sector information sharing hub, United States Computer Emergency Readiness Team (US-CERT), is a 2003 outgrowth of DHS's Office of Cybersecurity and Communications (CS&C). The US-CERT is currently the triage and information sharing branch of CS&C's National Cybersecurity and Communications Integration Center (NCCIC), which opened in 2009.[8] But ultimately it is DHS's Office of Intelligence and Analysis (I&A) that deploys field personnel to support the National Network of Fusion Centers (National Network), which accepts and shares threat data at the local level. The portals by which private sector entities receive and share threat data are often private sector-led information sharing and analysis centers (ISACs). While this construct has helped create a flow of cybersecurity threat information between and amongst public and private organizations, we believe that improvements are needed to bring their benefits to American SMEs, which often lack the resources (financial, time, and staff) to join and actively participate in ISACs. Moreover, most ISACs were created around U.S. government-designated critical infrastructure sectors,[9] and most of our members fall outside the siloed definition of an individual critical infrastructure sector or sectors. Executive Order 13691 created Information Sharing Analysis Organizations[10] (ISAOs) in part to alleviate this problem. Meanwhile, the market has responded to the need for timely cybersecurity information sharing, resulting in organizations that offer such information sharing services (and related cybersecurity threat mitigation services) as a business.

In practice, however, these efforts and initiatives—both government and private sector—have yet to make a meaningful impact on the small businesses that drive the digital economy's growth, innovation, and job creation, and many questions remain unanswered for our members. When an App Association member is hit with a cyberattack, with whom do they share it as the attack is occurring (as opposed to when a breach is discovered after the fact)? Somebody at NCCIC? Somebody at their local Fusion Center or an ISAC? Where are these entities located, and how should companies share threat information with them? While we note that the U.S. government has taken numerous steps to answer these questions, more can be done to educate SMEs like our members about them. For this reason, it is paramount that reinvigorated, enhanced federal outreach do more to communicate the answers to these questions to put us on the road to improving information sharing for small businesses.

Any private sector efforts to stand up an ISAC in the small business tech sector should be accompanied by federal efforts to improve the mechanics of information sharing. DHS should strive to make cybersecurity information that is shared user-friendly and understandable, and of the highest quality possible. We commend federal efforts in this respect (for example, NCCIC and US-CERT work on the Trusted Automated eXchange of Indicator Information [TAXII™], the Structured Threat Information eXpression [STIX™], and the Cyber Observable eXpression [CybOX™][11]). We also note that in a report issued on automated indicator sharing by the DHS's own Office of Inspector General (OIG) last week, the velocity and volume of threat information has improved.[12] This is a commendable improvement from 2015, when a report by Senator Tom Coburn, then-ranking member on the Senate Committee on Homeland Security and Governmental Affairs, found that private threat sharing centers were publishing, and patching, threats before US-CERT could even issue a warning.[13]

However, the OIG report also found that a few obstacles prevent the data US-CERT shares from being valuable and user-friendly. For example, the report noted that the pre-determined data fields limit the usefulness of threat data by restricting the descriptions of "specific incidents, tactics, techniques, and procedures that unauthorized users used to exploit software vulnerabilities."[14] We appreciate the tension between automating and standardizing how cybersecurity attacks are characterized with the diverse and dynamic nature of cyber-attacks; therefore, appreciating the value of TAXII™, STIX™, and CybOX™, we believe that DHS should also strive to permit cyber-attack reports to incorporate some flexibility and allow for the novel approaches attackers use to manipulate attack vectors and penetrate networks. Moving forward, we believe machine learning and artificial intelligence should be a critical tool to help make less structured threat information more useful for the private sector.

Unfortunately, our enemies are already using machine learning to orchestrate their attacks and evade less sophisticated defense measures. In order to prevent truly asymmetrical cyber warfare, our defenses must include cutting-edge methods and strategies, which, ultimately, the cybersecurity information sharing construct available to American SMEs should facilitate.

c. Publicize Best Practices that are Truly Scalable for SMEs

The NIST Cybersecurity Framework provides a scalable, flexible, voluntary toolbox that any organization can use to reduce vulnerabilities, prevent intrusions, and mitigate damage caused by cybersecurity attacks. However, our SME members often struggle with its detail and complexity, facing other (market-driven) priorities that do not allow them to fully leverage the Framework. Version 1.0 of the Framework is 41 pages long, and the draft of Version 1.1 is even longer, at 61 pages. Small businesses, even those in the tech sector, have precious little time and resources to get through dense documents, much less those that recommend consultation with large suites of risk management standards that often have expensive certifications associated with them.

Despite its complexity, we believe the Cybersecurity Framework is a comprehensive guide and should be the touchstone for efforts to enhance private sector efforts. Therefore, federal efforts around best practices must include references to the Framework and should center on simplifying its recommendations. We commend NIST itself, in recognition of this tension, for developing an SME-focused Framework fundamentals deliverable.[15] Further, the Federal Trade Commission (FTC) promulgates best practices in the form of its "Start with Security" guide for SMEs, which draws on the NIST Framework.[16] These SME-targeted efforts by NIST, the FTC, and other agencies are a great start, but as a nation, we have much work to do. Because bottom lines command business decisions, we suggest that such targeted education focus on making a business case (return on investment) for the use of the Framework.

We believe that this committee can directly assist the federal government's efforts to improve American SMEs' ability to manage cybersecurity risk through a new federally-funded national education campaign focused on improving SME cybersecurity risk management practices. Such education could help avoid the vast majority of cybersecurity breaches, which occur due to lack of basic cybersecurity hygiene. The Small Business Administration (SBA), with an infrastructure in place to reach SMEs in every region of the nation, would be well positioned to champion such a national campaign. As Joe Bonnell, the CEO of App Association member Alchemy Security in Denver, CO, aptly summarizes, "any capital allocated toward driving improved cyber hygiene within this constituency should include outreach programs through either regular lunch-and-learn activities through entities such as the SBA, or by funding user security awareness training similar to the "schoolhouse rock" campaign, which would provide tremendous investment leverage and could also be used to educate everyday Americans as well." The App Association commits to work with this committee to help create and shape such a campaign.

d. Facilitate Feedback from SMEs

The federal government should work with SMEs to understand the kinds of information sharing activities they are able to engage in and how to leverage federal information sharing resources.

Without a proper understanding of how small businesses are implementing the resources currently available, it is difficult to know what to do with the existing programs and frameworks to improve their accessibility and usability for SMEs. With adequate federal support, the Small Business Administration can assist NIST, DHS, sector-specific agencies, and other federal actors in gathering this input to inform future steps based on robust feedback from SMEs across all sectors as to which approach is most workable. The App Association is committed to assisting the federal government in understanding the unique challenges faced by the small business tech community.

II. The Statutory and Regulatory Environment Should Encourage SMEs to Effectively and Efficiently Manage Dynamic Cybersecurity Risks

a. Encryption and Law Enforcement Access to Data

Although encryption is not a complete solution by itself, it is an essential tool, especially for SMEs, to protect data. Any transaction involving data depends on TPMs, including end-to-end encryption (defined as a set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key), to maintain the integrity of data and ultimately the user trust on which our members' success depends. Any transfer of sensitive data—financial, health, etc.—requires that all available means be taken to provide for security and the integrity of the data. Encryption's role should not be understated—without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised.

Not only is the use of strong encryption a business necessity that every App Association member faces, but the U.S. government itself also currently plays an important role in promoting the use of encryption. NIST's Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.[17] NIST also provides the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards.[18]

Further, NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, lists HIPAA-related storage security needs, and describes the need to encrypt and decrypt electronic protected health information.[19]

Despite the important role encryption plays, various interests persist in demanding that "backdoors" be built into encryption for the purposes of lawful access. Mandating that "backdoors" be built into encryption for government access would not only degrade the safety and security of data, but it would also jeopardize the trust of end users. Backdoors are enticingly simple, but they are dangerously counterproductive—they create known vulnerabilities that any unauthorized parties can exploit. Undermining the technical proficiency of encryption moves us away from, rather than towards, legitimate policy goals such as law enforcement access to data.

Recent calls for "responsible" encryption simply are not responsible for your constituents or for our customers. This is a lesson we learned in the 1990s with the Clipper chip, which was a mistake that should not be repeated. "Responsible" encryption is just another word for broken encryption, especially when encryption can serve as a far better tool for crime prevention than investigation. We want to stop the bad guys before they act, and encryption can keep them at bay. We want to make data security for our customers and your constituents stronger, not weaker.

When investigations must take place, SMEs have been known to work well with local, state, and federal law enforcement officials. The App Association supports a collaborative approach between companies that retain customer data and law enforcement officials who seek access to it. To that end, legislation introduced in the House and Senate helps clarify when and how law enforcement may access communications data stored overseas using a warrant. The App Association strongly supports this legislation, the International Communications Privacy Act (ICPA, H.R. 3718 and S. 1671), and we urge members of the committee to cosponsor it. We will continue to look for opportunities to facilitate the mutually beneficial relationship between law enforcement agencies and SMEs in a manner that preserves the integrity of data security and encryption.

b. Liability Certainty for SMEs Seeking to Share Timely Cybersecurity Information

The Cybersecurity Information Sharing Act of 2015 (CISA) helped define private sector liability from sharing cyber threat data. As mentioned above, private sector information sharing efforts usually take place through ISACs or ISAOs. While only time will tell, the passage of CISA appears to have helped encourage more timely sharing by establishing liability protection for those responsibly sharing "cyber threat indicators," as long as personal information not directly related to the cybersecurity threat is "scrubbed." While CISA has provided some clarity, SMEs sharing cybersecurity information must take great care to meet these scrubbing requirements before they share. They cannot afford to absorb prolonged and expensive lawsuits like large multi-national corporations can in the event liability attaches to the sharing. Moreover, even though liability protections may exist, SMEs must also trust that those protections will apply to them in specific contexts. It takes time and effort to foster trust between SMEs and the federal regulators that can put them out of business for missteps. Practically, when such a question is presented to an SME's general counsel or outside counsel, it is much easier to simply say "no" than it is to engage in timely information sharing constructs and take on any liability.

Despite this reality, using DHS guidance for CISA compliance, more legal certainty exists for companies to share threat information, particularly through ISACs and ISAOs. However, as we discuss above, belonging to an ISAC or an ISAO often may present resource issues for SMEs (with a few exceptions).[21] We understand that ISAOs were developed specifically to fill the increasingly visible gaps between ISACs, as well as to permit other affiliations that may organically become attractive (e.g., based on location in a geographic region), but the ISAO standards process does face some criticism, and has not yet been completed. The App Association continues to educate its members on the legal issues associated with sharing cybersecurity information with other private entities and the government, and we offer our support to work with this committee and all stakeholders to further streamline the process.

III. Conclusion

We applaud the committee's attention to this issue and appreciate the opportunity to offer our perspective. Our ability to prevent cybercrime depends on how quickly we allow ourselves to move. Information sharing is central to quick action and requires close coordination between government, experts, and the private sector. If the conditions are right, our SME members will set the pace.

1- https://cloudblogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/
2- https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html
3- https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.
4- https://www.etsy.com/
5- https://www.etsy.com/legal/terms-of-use/#privacy
6- NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214final.pdf; see also 79 Fed. Reg. 9167 (Feb. 18, 2014).
7- https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi35bKX2bvXAhWD64MKHYuxA3cQFgg5MAE&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F4%2F6%2F8%2F4680DFC2-7D56-460F-AD41-612F1A131A26%2FMicrosoft_Cyber_Defense_Operations_Center_strategy_brief_EN_US.pdf&usg=AOvVaw1ax_GFcYWY67kEBbU4XbZp
8- https://www.us-cert.gov/nccic
9- https://www.dhs.gov/critical-infrastructure-sectors
10- https://www.dhs.gov/isao
11- https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.
12 -https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf
13- https://www.hsgac.senate.gov/download/?id=B92B8382-DBCE-403C-A08A-727F89C2BC9B
14- https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf
15- http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
16- https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
17- http://csrc.nist.gov/
18- http://csrc.nist.gov/groups/STM/cmvp/
19- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
20-https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
21-See https://www.fsisac.com/faqs#576