Committee on Small Business
Main Street Under Attack: The Cost of Crime on Small Businesses

Testimony of Graham Dufault
General Counsel
ACT | The App Association

Executive Summary

ACT | The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the domestic ecosystem ACT represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[1]

We applaud the Committee for its work examining the various threats faced by small businesses, including cybercrime. We often say that small businesses like our members are in the "Goldilocks zone" for cyberattacks, where they are successful enough to pay significant amounts to criminals but too small to fund a full civil case against their attackers. This position makes small businesses a prime target for cyber criminals, fraudsters, and scammers. According to Verizon's 2025 Data Breach Investigations Report, small businesses are nearly four times more likely than larger businesses to suffer a cyberattack.[2] Small businesses need help from you to ensure their businesses can stay operational through a cyber incident.

Our testimony today focuses on four key points:

- Cybercrimes are varied, but most are fairly low-tech and low-cost for bad actors. Nevertheless, these attacks cost businesses millions each year. Small businesses need support from Congress to safeguard against the disproportionate number of attacks focused on them rather than larger businesses.
- One key protection recently lapsed is the Cybersecurity Information Sharing Act of 2015 (CISA 2015). We support the reauthorization of this program with adjustments to account for today's threat landscape and to improve the accessibility of the program for smaller businesses.
- Even though small businesses are frequent targets of cybercrime, they also can provide important services to government agencies. Congress should support their work through proper funding for federal cybersecurity programs.

[1] https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf
[2] https://www.verizon.com/business/resources/Tf2d/reports/2025-dbir-data-breach-investigations-report.pdf

- Federal policies should continue to promote the use of technical protection measures like end-to-end and device encryption.

Cybercrime Methods and Costs

Although some cybercrime is committed using sophisticated technology, much of it relies on relatively low-cost tech and social engineering. For example, "smishing" scams, short for SMS phishing, employ text messages that appear to be from a trusted entity such as your bank or your employer. These messages are urgent and often contain fear-based messaging, urging you to click a malicious link, call a false phone number, or purchase gift cards and send them to the scammer. It only takes one employee replying to such a scam to compromise a business's cybersecurity.

Another common type of scam is called "Business Email Compromise," and it's exactly what it sounds like. Cyber criminals make spoof email addresses or websites, often similar to a real trusted account. They then request a standard business transaction, such as a change of mailing address or bank details, which either inserts the criminal's information directly into a legitimate business or plants malware on the target computer through malicious links. These attacks can also plant malware on a company computer if an employee clicks a link in the email.

Ransomware is a particularly common type of cyberattack targeting small businesses. Although 39 percent of attacks on larger organizations involve ransomware, an unbelievable 88 percent of attacks on small or medium-sized businesses involve ransomware.[3] In a ransomware attack, malicious software is imported onto a company network and used to completely shut down business operations. A criminal then sends demands to the business under attack, requiring huge sums of money to allow a return to operations. Unfortunately, many "Goldilocks zone" businesses find it easier to pay the ransom than attempt any kind of legal action while their business is inoperable. Without significant support for businesses to pursue such actions, this attack vector will remain lucrative for malicious actors.

These types of scams can cost businesses hundreds of thousands of dollars. According to IBM's Cost of a Data Breach report, the average cost of a breach in the United States in 2025 exceeded $10 million.[4] Although the cost on small businesses is generally lower—estimates range from $120,000 to $1.24 million for a cyberattack on small businesses—it is heavy enough to force bankruptcy and business closure. In 2020, more than 700,000 cyberattacks targeted small businesses, totaling $2.8 billion in damages.[5] Small businesses need congressional support to survive these attacks, including support for end-to-end encryption and sharing of cybersecurity information.

The Cybersecurity Information Sharing Act of 2015

---

[3] https://www.verizon.com/business/resources/Tf2d/reports/2025-dbir-data-breach-investigations-report.pdf
[4] https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91
[5] https://www.strongdm.com/blog/small-business-cyber-security-statistics#cost-of-cyberattacks-for-small-businesses

Importance of CISA 2015

Ten years ago, Congress recognized the importance of cybercrime prevention and passed CISA 2015. This law responded to several concerns of the cybersecurity industry, specifically antitrust issues related to the sharing of cyber threat information and cybersecurity best practices. Under previous law, this type of information sharing could be seen as collusion or violation of antitrust laws. CISA 2015 allowed businesses to improve their defensive posture through sharing information on cyber incidents, recent threat vectors they had seen from bad actors, and cybersecurity best practices they had developed. In the fiscal years covered by a recent Government Accountability Office (GAO) report, the agency found that tens of millions of cyber incidents were reported by the various federal agencies collecting information.[6]

Another key outcome of this law was the improvement of federal agencies' cybersecurity posture. Since a wide variety of federal agencies collaborated to gather and disseminate information on cyber threats, those agencies were better informed and better able to defend against cyberattacks using the information they gathered from businesses. The GAO report found that the development of automated information sharing tools helped agencies share both classified and unclassified information to better understand the threat landscape.[7] The strong success of the program was lauded by both Democrats and Republicans in Congress.

Despite the success of cyber incident reporting under CISA 2015, the law was allowed to expire on September 30, 2025. The law's overwhelming bipartisan support should have made for an easy reauthorization, but multiple attempts at passage in the House and Senate have failed. Recent reporting highlights the discomfort many businesses now feel about sharing cybersecurity information, as well as the resulting lack of information at the federal level.[8]

Areas for Improvement

Even with the general success of cyber incident reporting under CISA 2015, 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' Office of Cybersecurity and Communications (CS&C). Now US-CERT is the triage and information sharing branch of CS&C's National Cybersecurity and Communications Integration Center (NCCIC), which is now, as of 2018, a subdivision of the Cybersecurity and Infrastructure Security Administration (CISA). But it is DHS' 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 for private sector entities to receive and share threat data are often private sector-led information sharing and analysis centers (ISACs). However, small and medium-sized businesses usually lack the resources and wherewithal to join and participate regularly in ISACs. Moreover, most ISACs serve critical

[6] https://www.gao.gov/products/gao-25-108509
[7] https://www.gao.gov/products/gao-25-108509
[8] https://www.politico.com/news/2025/10/03/cyber-law-cisa-2015-shutdown-00592501

infrastructure industries, and most of our members fall outside the definition of critical infrastructure.

So, which arbitrary arrangement of alphabet soup is most important to a small business? When an ACT member company is hit with a cyberattack, whom do they share it with? Somebody at NCCIC? Somebody at their local Fusion Center or an ISAC? Where are these entities, and how should our companies share threat information with them? As with specialized legal and accounting functions, small businesses cannot be expected to maintain in-house cybersecurity expertise. But as Sebastian Holst, chief operating officer of our member company vFortified, points out, while small companies may be able to contract with IT firms to outsource cybersecurity services, they cannot transfer away cybersecurity risks from their business or outsource their own accountability. Sebastian also notes that we cannot expect small businesses to be able to effectively select and leverage outside cybersecurity firms without first having their own independent, working knowledge of cyber threats and information sharing best practices. Small companies will always have ultimate responsibility for the fallout from cybersecurity attacks and, as such, will always suffer the inevitable financial and reputational consequences that follow. And yet, while 46 percent of small business owners have experienced a cyberattack on their current business, only 23 percent of small and medium-sized businesses have a cyber readiness plan they are very satisfied with.[9]

Organizations like the Cyber Readiness Institute provide meaningful materials for small businesses and there is a role for government as well. If federal outreach can help simplify and streamline the learning curve for non-expert small companies, they will be in a better position to secure their businesses, their partners, and of course their customers. Improving small company awareness brings us further down the road to improving information sharing overall to better protect our local economies from threats both here and abroad.

Small Cybersecurity Businesses Help Protect Federal Agencies

One way that the Cybersecurity and Infrastructure Security Agency (CISA) has fulfilled its mandate is by providing cybersecurity services to other federal agencies. With millions of devices across country, the federal government is at significant risk for cyberattacks. And the prize available to cybercriminals who successfully penetrate federal systems is enormous: troves of sensitive information on persons all over the country, access to power grids and fuel sources, and personal correspondence of key government officials.

CISA has provided cybersecurity services to other agencies to decrease these potential vulnerabilities, including a program for mobile app vetting (MAV). This program vetted mobile applications for security concerns, malware, and other vulnerabilities before allowing them to be downloaded to federal government-owned devices. ACT member company Quokka was responsible for the operation of this program, using their vetting technology to investigate up to

[9] https://www.mastercard.com/us/en/news-and-trends/stories/2025/small-business-cybersecurity-study.html

10,000 apps every month. Their work saved the government unknowable amounts of money in manpower and consultant fees. And although the program received high praise, funding cuts beginning in fiscal year 2024 have endangered CISA's commitment to mobile app vetting.

Continued cuts to CISA's budget and staff turnover at the agency have combined to stall this program's renewal. Without it, federal devices will be less secure, cyber threats will go undetected, and the government will end up spending more money than the cost of the program for a potentially disastrous result. We urge Congress to provide full funding for CISA's programs, including MAV.

The Importance of End-to-End and Device Encryption for Security

Although encryption is not a complete solution by itself, it is an essential tool to protect data, especially for small businesses. App makers rely on the trust consumers have in their devices and software. Especially in the mobile space, consumers take their most sensitive data with them everywhere on their secure mobile devices. The ability to encrypt these devices without a third party maintaining a separate key or vulnerability is an important aspect of continuing down the path we are on now to unlock the potential of smart devices to handle our finances, manage our health information, and access work. Mandating that messaging providers build "backdoors" into end-to-end encryption—or that device makers keep separate vulnerabilities for device encryption—for the purposes of government access would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. The existence of mandated vulnerabilities make the business prospects for cybercrime much more attractive. Hackers might spend hours or days trying to determine if a vulnerability exists at all and then might give up if they think there is no way in. But if they know it has to exist because the law mandates it, suddenly the resource investment of attacking the service is worth it—and eventually someone will discover it.

Occasional calls for "responsible" end-to-end or device encryption are simply not responsible for your constituents and ACT members' customers. This is a lesson we learned with the Clipper chip, which was a mistake that should not be repeated. "Responsible" encryption is just another word for broken encryption. The Federal Trade Commission describes encryption of sensitive customer information when transmitting it as a "basic step" to maintain security, confidentiality, and integrity of customer information for financial institutions.[10] Similarly, the Department of Health and Human Services in its Health Insurance Portability and Accountability Act (HIPAA) rules make encryption an "addressable implementation specification" that must be implemented if, "after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard . . ."[11] Weakening encryption to facilitate investigations would also facilitate the success of criminal hackers and limit our ability to keep them out.

---

[10] https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
[11] https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html

Laws under consideration in Sweden and the European Union would compromise the security of encryption by requiring companies to scan, report, and remove harmful content, including encrypted communications. Sweden's rule would compel service providers to store, and give law enforcement access to, user communications, including those protected by end-to-end encryption. The United States must not follow their lead and weaken one of the most effective tools for preventing cybercrime. Weakening protections like encryption and authentication doesn't make people safer; it makes them more vulnerable to identity theft, financial fraud, blackmail, account takeovers, and stalking. And for smaller companies, the costs of compliance with such requirements could be so high that they are pushed out of the market entirely.

Conclusion

We applaud the Committee's exploration of 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 this requires close coordination between government, experts, and the private sector. If the conditions are right, small companies like ACT members will set the pace.