NATIONAL
CYBERSECURITY
ALLIANCE

Written Testimony of Lisa Plaggemier, Executive Director of the National Cybersecurity Alliance (NCA), before the House Committee on Small Business

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

December 2, 2025

Chairman Williams, Ranking Member Velázquez, and distinguished members of the House Committee on Small Business, thank you for the opportunity to provide testimony on how cybercrime affects small businesses across the United States. I greatly appreciate the Committee including cybersecurity and cybercrime in this discussion.

The National Cybersecurity Alliance is a nonprofit on a mission to educate people on avoiding cybercrime, scams, and fraud. From families to Fortune 500s and every kind of organization in between, we work with one goal in mind: to make cybersecurity easier and more accessible, so that we can experience the benefits technology brings to our lives without the worry of being victimized.

We reach millions of people with Cybersecurity Awareness Month every October (we are the founders), and campaigns on topics ranging from AI deep fakes, to avoiding scams like pig butchering, crypto, and romance scams. We inspire good cyber habits, like using a long, unique password on every account, and multifactor authentication (MFA) on every account that offers it.

We convene security leaders in the private and public sectors to help protect Americans from cybercriminals, transnational organized crime gangs, and nation-state actors. We are an alliance - a reminder that creating a secure online world is a group effort.

I haven't always worked in cybersecurity. I spent the first 15 years of my career in a large enterprise working with small businesses: automotive dealers and distributors. I learned firsthand the importance of small businesses to their communities, the value of partnership between the factory and the franchise, how a well-managed business can thrive and be resilient creating generational wealth, and conversely, how brutal competition, 50% employee turnover, and poor management and cyberthreats can cause a small business to fail, with ripple effects across a community.

Cybersecurity is not just a technical issue – it's a business risk that small businesses need to manage through people, process and technology. The majority of security incidents are not technology failures, they're people and process failures. Many incidents have poor basic IT management as their root cause, like employees using the same passwords on multiple accounts, not using multifactor authentication (MFA), operating systems that are out-of-date and vulnerable, software that goes unpatched, a lack of employee training on phishing and other threats, and poor offboarding of employees when they leave the company, failing to remove their access to data and systems.

You could view these types of failures as technology failures, because technology largely hasn't been designed to allow for human error. But until that happens, we, as users of technology, need to be educated in our use of tech, and businesses need to manage the risk to survive and thrive. Many of the companies that sit on the Board of the NCA provide security products and services to SMBs and most will tell you the same thing – it can be very difficult to convince a small business owner that he/she should operationally prioritize cybersecurity. Small businesses are very busy, with competing priorities.

There are five myths that we regularly hear from small businesses:

Myth: "I just don't think I'm on the radar of the bad guys."

According to Mastercard's Global SME Cybersecurity Landscape Report, 46% of SMBs say their business has experienced a cyber incident; according to a survey from the Identity Theft Resource Center (ITRC), the number is 81%. Most of these businesses experienced multiple attacks, with threat actors deploying increasingly sophisticated methods, including AI-powered attacks cited as a root cause in more than 41% of incidents.

Businesses with fewer than 100 employees are now 2.5x more likely to be targeted than those with 500+ employees (*source: SC Magazine*). Seen as easier targets by cybercriminals, employees of small businesses experience 350% more social engineering attacks than large companies.

More than half of the affected businesses reported losses between $250,000 and $1 million. While many are drawing from cash reserves or relying on cyber insurance proceeds, a significant portion – nearly 40% – are raising prices on their goods and services, in effect creating a cyber tax that we all pay. (*Source: ITRC*)

Small business are also heavily targeted by scammers because they lack the protections and monitoring large companies use to hunt brand abuse – large organizations monitor for fraudsters abusing their brand in phishing emails and scammers using AI to quickly create look-alike websites used to deceive customers. According to Visa, "fraud has evolved from being opportunistic — it's moved to strategic, automated, and scalable. Criminals operate with R&D cycles, go-to-market strategies, and continuous improvement processes. We're entering an era where nothing can be trusted at face value. AI enables the creation of synthetic content — fake merchant websites, fake identities, fake conversational agents...that is indistinguishable from legitimate business materials." My hypothesis is that the criminals have adopted AI faster than most small businesses, in order to impersonate small businesses and scam victims more efficiently.

Myth: "We don't have anything of value to cybercriminals."

From my automotive experience, I know that the average car dealer has 50,000 consumer records that include SSNs, driver's license numbers, customer employment history and more. Each one of those consumer records is worth hundred of dollars on the dark web. Additionally, with the onslaught of ransomware, the fact that your business exists makes you a target. According to the 2025 Verizon

Data Breach Investigation Report, 88% of SMB attacks last year involved ransomware. A ransomware attack can take a company offline for two to four weeks, and cost thousands to hundreds of thousands or millions in remediation, recovery, and lost revenue. Customer trust can take years to rebuild.

Small business intellectual property (IP) is also very valuable to nation-state actors like the People's Republic of China (PRC). There are multiple examples of SMBs operating in highly specialized niche markets whose businesses have been threatened, or been driven out of business, when their IP was stolen by the PRC who then spun up a low-cost competitor, producing the same highly-specialized product at a fraction of the cost because they had made no investment in the IP. American small businesses can't out-spend a foreign competitor who acquired the same technology at zero cost.

This is also a factor for entrepreneurs. If small innovative firms can't protect their IP long enough to commercialize it, the US becomes less competitive and innovative.

I've met a small business owner who is the only manufacturer in the US of a piece of equipment necessary to road paving who had no understanding of the risk of IP theft to his business, literally saying, "Why would a cybercriminal attack us?"

I've met a small business in a highly specialized segment who unknowingly employed a Chinese spy for years. They didn't know it until the spy went to work for a large enterprise that had an insider threat program that detected the epionage quickly. The Chinese national was convicted and is currently in federal prison. The small business still doesn't know what IP was stolen from them because they had no monitoring or logging in place at the time they employed him.

According to the Verizon Data Breach Investigation Report, espionage-motivated breaches now make up 17% of all security incidents. And state actors increasingly target small businesses because they are entry points into larger supply chains. Russia and China patiently make multiple hops through smaller companies to get to their desired large target.

Myth: "I've got a guy", i.e., an IT person or Managed Security Services Provider

If you are a small business owner, cybersecurity is not someone else's job: it's yours to manage. In our experience, small business owners don't know enough about cyber to manage it as a function of their business. They know enough about finance, for example, to have a meaningful conversation with their accountant, but the same is not true with their IT provider, whether it's an employee or an external provider.

They may not have known what questions to ask when hiring or contracting for that service. They might not know what metrics they should be asking for to track progress on protecting their business. They may have knowledge gaps on best practices for patching, resiliency planning and exercises, data handling, access and identity management, employee security training, and other basic IT practices. Their businesses often lack written IT policies, so they have nothing to manage *to*.

- 75% have no regular cybersecurity training program
- 80% don't implement multifactor authentication

- 80% have never conducted a vulnerability assessment
- 53% have no formal incident response plan
- 55% lack endpoint protection
  Source: TotalAssure

These aren't technology failures, this data is evidence of management failure. The National Cybersecurity Alliance believes small businesses don't manage what they don't understand, and our *CyberSecure My Business* program educates owners and operators, using business terminology they can understand so they can better manage cyber risk.

Myth: "My technology vendor/cybersecurity insurance takes care of it."

Small business owners are traditionally hands-on managers, except when it comes to cybersecurity. We believe it's the lack of knowledge that leads to some small business owners failing to manage the risk and assuming it's someone else's job. Many technology vendors now have protections in place, many without an up-charge, but the business needs to properly configure them. A technology vendor may offer MFA, but it's up to the business to enable it and train their employees on the proper use. A technology vendor may offer secure cloud storage, but again, the business needs to properly configure it, and employees need to use it and not go around it because it's "inconvenient."

Cyber insurance is not a panacea. Claims can be denied for your own IT negligence, often based on policy exclusions for human error, outdated security, or failure to follow security protocols. Many policies require you to meet certain security standards, and if a breach results from a failure to meet these requirements (such as inadequate security measures, poor employee training, or a lack of an incident response plan), the insurer can deny the claim.

Myth: "Cybersecurity is too expensive. My IT person/provider just wants to spend my money."

Many of the most effective measures involve people and process protections that cost little to nothing to implement, if businesses will take the time to manage them. For example,

- Proper vetting and onboarding of new employees
- Written policies and procedures with annual employee training and acknowledgement of the policies, including acceptable use of technology policies on passwords, MFA, email, internet, and social media use
- Access controls; rule of least privilege for CRM and other systems – who gets access, why do they get access, what are they accessing, and when are they accessing it
- Third-party risk management and access management
- Proper offboarding of employees, revoking access to systems

Again, there is a failure of education and lack of clear communication between the business owner and their IT provider. One example I heard at a car dealership involved an end-of-life PC in the parts department running WindowsXP, introducing vulnerabilities into the dealership environment. When the IT manager asked the owner to replace the PC, the owner said, "the parts manager says it still works just fine," declining to make the investment. The failure was a lack of communication on the amount of risk to the business that old PC presented.

As outlined in our five myths, the ITRC report found that there is a dangerous disconnect between the perceptions of risk and the adoptions of basic security controls, such as MFA.

We believe that public-private partnerships are an effective and efficient way to help small businesses learn to better protect themselves. According to our *Oh Behave! Report on Cybersecurity Behaviors and Attitudes*, most people don't turn to the federal government for advice and guidance; they look to private sector companies, vendors, and nonprofits like us for guidance. Our *CyberSecure My Business* live-taught remote course includes six modules:

1. Why Cybersecurity is important to your business
2. Managing the security of your people and your money (business email compromise)
3. Managing who gets access to what (access rights and passwords)
4. Managing the security of your systems (updates and patches)
5. Ransomware and backups; managing your MSP/vendors
6. Managing incidents: Planning, insurance and next steps (incident response)

Eighty-nine small businesses have taken the course, but only 43 attended at least four of the six sessions and assignments. It is a challenge to pull owners away from their operations, even for 60-90 minutes a week, without some incentive. We have 371 small businesses on our waitlist, and are always seeking funders to cover our costs.

Of those who completed the course & provided feedback:

- 88% said that they are now more aware of their specific business assets that cybercriminals would target, and that they now feel more comfortable responding to a cybersecurity incident affecting their business.
- 83% said they feel more comfortable engaging with IT staff or cyber vendors on the topic of cybersecurity for their business.

As a result of the training, the course participants reported implementing or making plans to implement:

- Staff training on scams and phishing
- MFA
- A regular patching schedule
- Regular data backups

These figures motivate us to widen the funnel, attract more attendees and incentivize attendance, because if business owners attend, they are highly likely to implement real changes that reduce their risk and make them more resilient.

Cybersecurity does not have to be as intimidating and confusing as people perceive it to be (*source: Oh Behave!*). Education works! Strengthening small business cyber resilience strengthens U.S. supply chains, exports, and competitiveness against foreign adversaries. We stand ready to work with federal agencies to better educate small business owners how to avoid being victimized by cybercrime, IP theft, and scams, whether it’s opportunistic cybercrime or sophisticated nation-state actors. Through partnerships like cooperative agreements between nonprofits and government, we can work more efficiently and effectively than government can alone. We are stronger together.

I would like to thank the Committee and offer our ongoing partnership to support America’s small businesses.