Testimony Before the U.S. Small Business & Entrepreneurship Committee
Cyber Crime & Existential Threat to Small Businesses
Stacey Smith, CEO, Cybersecurity Association of Maryland, Inc. (CAMI)

Thank you. I am Stacey Smith, CEO of the Cybersecurity Association of Maryland, Inc., or CAMI for short. CAMI is a statewide, nonprofit organization based in Baltimore with a mission of sales generation and job creation through Maryland's cybersecurity industry. Our members include almost 450 of Maryland's cybersecurity product and service companies, many of which are small companies focused on helping small businesses be more cyber secure.

In 2017, the Better Business Bureau conducted a national study and published the "State of Cybersecurity Among Small Businesses in North America" report. 85% of the businesses surveyed had 50 or fewer employees and were in various industry sectors including retail, construction, financial, manufacturing, real estate, healthcare and others.

The research found that small businesses are becoming more aware of cyber threats and are taking proactive steps to enhance their cybersecurity. In fact, 9 out of 10 said they have some form of cybersecurity in place with the most common being antivirus and firewalls.

But that's not nearly enough to ensure a business is safe from today's advanced cyber threats. As a result, they leave themselves vulnerable, and may even lose more through a cyberattack than they would have spent implementing cybersecurity protections to prevent them.

If small businesses are more cyber aware than ever, why aren't they doing more to protect themselves, their data and their customers? The BBB's research found that companies are ill-equipped primarily due to a lack of resources, including funds, and the lack of knowledge – what to do, who to consult or hire.

Here are a few real cyberattack examples provided by some of our members:
A small marketing firm in Baltimore was hit with a ransomware attack. Everything on their server including client documents, financial spreadsheets and the project tracking software at the core of their day-to-day business were locked and held for ransom. Hackers used automated bots to search the internet for vulnerable servers without the necessary security controls. When the bots reached the agency's server, they hit pay dirt. The agency reached out to a MD cybersecurity company that restored their systems and 317,000 files had to be painstakingly restored. Two days of client work were lost. It took four days to fully restore everything, and the business spent thousands of dollars to mitigate the situation.

In another example, the CFO for a small MD construction company fell target to an email phishing scam. He received a message from what looked to be one of their regular payees asking him to update wire information and transfer money. He did so. Seeing a vulnerable target, the hacker sent another message that ultimately allowed access for a ransomware attack through which the company's files were locked until the company paid the ransom money. In total, the company lost almost $200,000 through the wire transfer, ransom payment and cost for a MD cybersecurity company to completely restore and rebuild their network.

Lastly, another recent example - a small organization noticed anomalies affecting the CEO's electronic calendar and documents and reached out to a MD legal firm for help. The firm's data security breach response team's investigation revealed that the organization's recently-fired head of Information Technology had hacked back into the organization's systems and deleted key events and documents of the CEO and exfiltrated electronic personal health information of thousands of Marylanders. The US Attorney's Office and FBI were notified. The hacker was charged and sent to prison. The legal firm helped the organization notify affected individuals.

Had these businesses had proper protections and employee training in place, it is possible that the cyberattacks could have been prevented or mitigated saving them from immeasurable stress; time, production and financial losses; and even reputational damage.

But as previously mentioned, small businesses often don't know what help they need or where to go for help, and the fear of the cost keeps many of them from investing in cybersecurity before they are faced with a cyberattack.

Luckily, for MD businesses, CAMI exists to connect them to companies within our state with answers to their questions and products and services they need to be cyber secure.

They can connect online through our directory of MD cybersecurity providers (www.MDcyber.com/listings). They can also attend events, including our upcoming MD Cyber Day Marketplace, to connect face-to-face with local cybersecurity companies.

If funding is the issue, our state legislators passed a nationally unique BIPARTISAN bill in 2018 making it more affordable for businesses to be cyber secure.

This bill provides a tax credit for MD businesses with 50 employees or less for 50% of what they spend on cybersecurity products and services purchased from a Qualified MD Cybersecurity Seller - up to a total tax credit of $50,000 annually. In 2019, we have $4 million to award in tax credits to small businesses through this program.

Our organization has partnered with the MD Department of Commerce, the Better Business Bureau of Greater Maryland, Regional Manufacturing Institute of Maryland, MD Manufacturing Extension Partnership and others to make small businesses aware of the tax credit program to incentivize them to be proactive rather than reactive in their efforts to be cyber secure.

This buy-local bill provides a tool for Maryland cybersecurity companies to generate local sales, grow and ultimately add jobs as they do so, and it incentivizes MD businesses to purchase the cybersecurity products and services they need, thus ensuring a more cyber secure business environment in Maryland.

Thank you for the opportunity to testify. I am happy to answer any questions you may have.

stacey@MDcyber.com, (443) 844-0047, www.MDcyber.com