Testimony of: Dr. Shawn P. Murray

President of Murray Security Services and
President Elect of the Information Systems Security
Association International Board of Directors

Before the United States Senate
Committee on Small Business and Entrepreneurship

"Cybersecurity: Challenges and Opportunities for Small Businesses"

Field Hearing

August 15, 2023

Senator Hickenlooper, Chairman Cardin and other members of the Committee, thank you for this opportunity to address an area of national interest addressing cybersecurity concerns for small businesses in the United States. As a practitioner and educator, it is my intent to make you aware of some very important information which can be used to influence decisions related to information privacy and cybersecurity.

Today, we know that 80% of most organizations business processes are automated, meaning that we are using some type of technology to process, transmit or store information related to a job task that are performed by employees. There can be risk associated with these processes if the employees and business managers don't consider security as part of awareness. The following statistics associated with cybersecurity trends for small and mid-sized businesses include:

According to the National Cybersecurity Alliance, 70% of cyber-attacks target small to mid-sized businesses. The Ponemon Institute reports that the average cost of a breach for small and midsized businesses is 383k and according to the Better Business Bureau, 50% will become unprofitable within a month of being breached. Finally, Gartner published in its Top Trends in Cybersecurity 2023 report that 60% of small businesses that are victims of a cyber-attack go out of business within six months and overall, cybercrime costs small and medium businesses more than $2.2 million a year.

In the 2023 Data Breach Investigations Report, Verizon reported that:

- "Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24% of breaches. Of those cases, 94% fall within System Intrusion."
- "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering."
- "83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches."

The Corona Virus Pandemic saw a significant increase of remote workers and an investment of online technology, remote meeting applications and cloud-based business resource subscriptions. The initial focus of small businesses was to get connected to resources. Unfortunately, security was often not considered until the business began experiencing data breaches, interception of remote meetings and unauthorized disclosure of sensitive information on non-company owned devices. While cloud and remote computing have increased productivity and business capabilities, they have increased the cyber attack terrain.

In the last two years our team performed assessments on small and medium sized businesses in multiple industries and in multiple states across the country. Some of the top issues we have seen include:

- Social engineering people to disclose things like user names and passwords, sensitive product information and personal identifiable information
- Lack of dedicated IT or cybersecurity resources
- Uncontrolled access to sensitive areas of a building.
- Sensitive information found in trash cans, dumpsters and in unattended workspaces.

- Computer applications or equipment that are vulnerable to cyber-attacks due to missing patches or misconfigurations.

Cybersecurity is primarily about protecting information. Some of the most sensitive information that needs to be protected is privacy information. This means that relationship between cybersecurity and privacy data and information is significant. While the United States has many various privacy laws related to highly regulated industries like banking & finance as well as healthcare, we do not yet have an overarching national privacy law such as the General Data Protection Regulation in the EU. A current bill being considered called the "Safe Data Act" would address many areas. Instead, businesses have to navigate the complexity of 50 states privacy and cybersecurity laws which can become overwhelming and time consuming.

The United States provides one of the largest procurements of small business resources. To be considered, businesses now have to comply with cybersecurity hygiene requirements as identified by FedRamp, the Cybersecurity Maturity Model Certification (CMMC), NIST SP 800-171 Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations as well as other requirements identified in the Federal Acquisition regulation.

Small businesses need access to free resources for education and training to understand these requirements.

Based on recently passed legislation, SBDCs now require a cybersecurity lead center to support their small business clients to help address cyber issues. SBA should require additional dedicated funding to better develop standardized programs across SBDCs and SCOREs for consistent Training & Education as well as cyber related resources to help protect small businesses. An example is the America's SBDC North Star program which represents the overarching efforts of the America's SBDC network to mitigate cyber threats to small businesses. Dedicated funding would allow consistent cyber programming instead of having to chase funding through grant proposals each year.

An additional resource to consider is the Center for Internet Security (CIS) which provides CIS Critical Security Controls and Benchmarks for prioritized set of actions to protect organizations and data from cyber-attack vectors.

For small businesses the three primary areas to focus are:

- Security Awareness and Skills Training, Data Recovery and Access Control Management

The National Institute of Standards and Technology provides additional guidance and resources as discussed in Mr. Stein's testimony.

In closing, cyber threats pose a significant challenge to our country, our businesses and to our national security. A disruption to commerce due to threat actors attacking businesses should be considered a serious threat to our economic viability. With the onset of new technological advances such as Artificial Intelligence and the Internet of Things, there needs to be dedicated resources to educate, train and advise business owners and leaders on achieving appropriate cybersecurity hygiene to protect their business as well as their information.

Again, thank you for this opportunity to testify in front of this committee.

Resources:

Center for Internet Security (CIS) - https://www.cisecurity.org/controls

2023 Data Breach Investigations Report - https://www.verizon.com/business/resources/reports/dbir/2023/small-business-data-breaches/

Gartner Identifies the Top Cybersecurity Trends for 2023 - https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023

The Ponemon Institute - https://www.ponemon.org

Better Business Bureau - https://www.bbb.org/

North Star Program: Cybersecurity Guidance For Small Businesses - Https://americassbdc.org/cybersecurity/