Testimony before the U.S. Senate Committee on Small Business and Entrepreneurship

Gina Abate
President and CEO, Edwards Performance Solutions

Preparing Small Businesses for Cybersecurity Success

Thank you Chairman Risch, ranking member Cardin, and members of the committee for the opportunity to testify today. I am Gina Abate, President and CEO of Edwards Performance Solutions, a Woman Owned Small Business, as well as the Chair of the Board for the Cybersecurity Association of Maryland, Inc. (CAMI).

The high risk of financial damages is an unprecedented challenge to small businesses, intensified by the fact that the vast majority are unprepared to properly protect their assets. Discussions with hundreds of small businesses by CAMI members demonstrate a clear pattern of inaction, with the most frequent explanations being:

- “My business is small, I’m not a target.”
- “Cybersecurity is expensive and I can’t afford it.”
- “I’m not a regulated business, so I don’t need to worry about it.”

Let’s address these justifications. Attackers are targeting small businesses with increasing frequency and sophistication. If an attacker is able to compromise a business system, they can use that access to exploit business information, attack business customers and suppliers, and may even shut down business operations entirely. For an attacker, any foothold is a good foothold.

So, what should a small business do to start their cybersecurity program?

Every business should invest the time to understand the value of their assets, engage experts to understand the vulnerability of their IT systems, and take appropriate steps to manage their cyber risk. The more valuable their assets and the weaker their ability to detect, stop, and mitigate cyber damages, the greater the risk.

The absence of regulation should not be the driver for a cybersecurity program. In fact, regulatory compliance should be an outcome of a well-structured security program, not the reason for it. Small businesses who adopt a framework, like the NIST Cybersecurity Framework, are able to implement a cybersecurity and risk program to address current regulations, as well as any new regulations, with minor program changes.

Cybersecurity is a continuous process, not a one-time event and best approached using proven methods. I recommend the NIST Cybersecurity Framework in conjunction with the guidance of expert cybersecurity practitioners. Small businesses must implement a culture of safety – leveraging employee situational training and low-cost tactics like enforcing proper passwords, encrypting hard drives, and limiting user ability to load undesirable software.

The concepts of the NIST Cybersecurity Framework are straight forward, but in practice, organizations become overwhelmed with information. It is important to note that organizations do not need to address all cybersecurity concerns at once. In most cases, a prioritized approach is sufficient to ensure key systems and/or business units are protected before addressing secondary areas of concern.

Even with the best protection tools and procedures in place, cybersecurity risk is not eliminated. Continuous monitoring is required to quickly detect malicious, undesirable, or abnormal activity. Once a breach is detected, an immediate response is critical. Businesses must have an exercised and maintained plan in place during “peace time” to ensure business damage is minimized, with the necessary actions and resources established to regain client trust.

It is imperative the small business community understands cybersecurity is critical to overall business success. The challenge lies in convincing small businesses of the urgency to do more in protecting their assets. The compromise of one business can often impact suppliers and customers; there is much more at stake than the failure of one business at a time.

But, how do we incentivize small businesses to start preparing? In Maryland, the bi-partisan Cybersecurity Incentive Tax Credits Bill (SB228) made Maryland the first state to incentivize small businesses to purchase local cybersecurity protections and investors to advance Maryland cybersecurity companies. Those of us at CAMI are especially excited because thousands of small Maryland businesses at risk of cyber damages can now get the help they need at lower cost.

Thank you again for the opportunity to testify. I look forward to discussing this topic with you further.

Gina Abate – Bio

Gina Abate is the President and CEO of Edwards Performance Solutions (Edwards), a Woman Owned Small Business (WOSB) helping organizations achieve secure operational performance. Gina’s strong leadership and industry knowledge enables strategic plan development for growth and to advance the company’s mission. Under her leadership, Edwards expanded its offerings to include cybersecurity and IT services, complementing a strong enterprise management and training history.

Ms. Abate is also the Board of Directors Chairperson for The Cybersecurity Association of Maryland, Inc. (CAMI). She is featured in multiple publications promoting cyber awareness and was recently recognized by The Daily Record as one of their “Most Influential Marylanders” for her contributions to current and emerging technology.

Prior to joining Edwards, Ms. Abate was a Vice President at NTT Data Federal Systems (formerly Keane Federal Systems) and BAE Systems. She has 30+ years of proven leadership with executive, technical, and business management experience in the Federal Government as a Civil Servant and a commercial sector contractor.