States Confront the Cyber Challenge

Small Business and Cybersecurity

The Threat to Small Businesses

Virtually any small business relies on technology and an Internet connection to thrive in today's hyper-competitive, digital economy. Consequently, small businesses across the United States, who store financial and personal data on millions of Americans, present rich targets for hackers. As larger companies adopt more advanced cybersecurity, criminals are ramping up attacks on the smaller firms that do not prioritize data security or lack the resources to protect their digital assets. The direct and indirect costs of these attacks can threaten closure for some. Yet security in small businesses is not just a matter of economics, but also of national security. Many larger corporations, including defense contractors that hold highly sensitive data, contract with thousands of third party vendors. A sophisticated attacker can compromise these small businesses and exploit their trusted position to infiltrate far more heavily defended organizations. But small business development is fundamentally a state and local issue, and governors have a critical role in this space.

Ongoing Challenges to Improving Security in Small Business

Too many unknowns: Many small businesses operate without any dedicated IT staff. They do not know the range of threats or the proper resources to consult. In many cases, they do not know that their systems have been compromised until notified by an outside party. Owners who understand the threat may find it difficult to navigate the complex array of resources and software solutions.

Limited resources in a competitive environment: Many small businesses operate on very thin margins. Owners devote substantial time and resources to minimizing costs so that they can compete in their sector while maintaining profitability. In this environment, small businesses frequently view cybersecurity measures as a luxury they cannot afford.

Fear of liability: Business owners who understand cyber risk may nevertheless hesitate to report attacks; even limited regulatory action or private litigation could drive them out of business. This frustrates efforts by law enforcement to identify trends in computer crime and craft resources for businesses who have yet to fall victim to the most prevalent scams.

Regulation is not feasible: States and localities do not want to increase the cost of doing business by instituting mandatory cybersecurity standards. Businesses that are already regulated can mistakenly believe they are secure just because they are compliant.

Recommended Steps for Governors

Use security incentives: Business owners are more likely to adopt better security practices if they believe it will be good for business. Governors should work with legislators, insurance commissions, and business groups to design tax and insurance incentives that persuade otherwise disinterested businesses from adopting cybersecurity measures.

Consolidate and disseminate training materials and guidance: Federal agencies and private associations already publish useful security information, but it does not make it into the hands of small business owners. Governors should convene these actors to consolidate duplicative products into a smaller set of authoritative documents, certified by the state. States should actively engage local and regional business associations to disseminate the recommendations and conduct hands-on demonstrations.

Work with industry and law enforcement to improve reporting mechanisms: Many small businesses have information on cyber attacks that is of great value to law enforcement. The public and private sectors should work together to develop an anonymous reporting mechanism that provides state agencies with evidence of criminal activity, without outing businesses that have suffered a breach.

Identify private partners to offer pro-bono assistance: Small businesses have expressed a need for a list of approved security vendors, but building such a resource would be fraught with political and administrative difficulties. Instead, governors should engage IT, cybersecurity, and legal services companies who would be willing to offer limited pro bono services to small businesses that need help implementing defenses or responding to attacks.

Use cyber talent programs to provide low-cost assistance: States are pursuing innovative workforce development programs, many of which place students and recent graduates in cyber apprenticeships. These initiatives could loan participants to nearby local businesses in need of basic assistance with cyber preparedness.

Support small business cyber centers: Recent national legislation has directed the Small Business Administration (SBA) and the Department of Homeland Security (DHS) to assist small businesses in improving cybersecurity. Governors should build relationships with SBA and DHS policymakers as they craft and implement their strategy.

Please e-mail Timothy Blute, Program Director, Homeland Security and Public Safety Division, NGA at: tblute@nga.org *with any questions.*