Small Business Cybersecurity
and the Global Supply Chain

Questions to Consider:

- Are you and your business partners taking the proper precautions to secure your business sensitive data?
- What type of data do you share with your suppliers? Is all of the data necessary?
- What type of interdependencies does your network have? How are all points in that information chain secured?
- Should your company consider cybersecurity insurance?
- Who has access to your data? Is their access essential to their job?

Adam W. Salerno

Adam W. Salerno is Executive Director for Global Supply Chain and Trade Facilitation at the U.S. Chamber of Commerce.

U.S. CHAMBER OF COMMERCE

AMERICA'S SBDC FLORIDA

How it Works

More often cybersecurity and supply chain are being talked about in the same sentence, as they have both risen to C-suite priorities over the last decade. And for good reason—both are critical to the competitiveness of thriving businesses. Manufacturers import and export parts and supplies from around the globe. Retailers, pharmaceuticals, e-commerce, and others all thrive on a supply chain that propels their products to consumers. Millions of businesses, moving billions of dollars worth of products daily in a just-in-time delivery environment, are all linked by an information exchange that could be vulnerable.

In a world where digital networks are equally as important as physical networks, it is critical for small business to be vigilant with the cybersecurity of their supply chains.

Why Small Business Should Care

When we hear about major data breaches, we do not always think about small businesses. However, they are more often the target of cybercriminals because they are viewed as the weakest link to exploit for vulnerabilities. Information is not only taken from your system, but can be used to infiltrate an entire network within the supply chain[1]. We have seen time and time again that many of these larger data breaches starting with a supplier, a maintenance company, or even a contractor have led to a broader network breach impacting the entire supply chain.

More than 95% Florida's exporters are small businesses. With so small businesses using supply chains to access the globe, it is imperative to engage your business partners to develop procedures and address cybersecurity risks together. If there is weakness in your network of suppliers your company's critical data could be at risk.

What Hackers Are Looking For

The cost of a breach could be tremendous for a company from the loss of consumer data, commercially sensitive information, financial information, or intellectual property rights. Put simply, a breach could lead to the release of information that could materially damage a company or even put it out of business. That original breach could have come from anywhere in the supply chain not necessarily your own system. Company leaders need to consider what information they share with partners in the supply chain and ensure that everyone is taking the proper precautions to secure it.

1 Small Business Administration. *Introduction to Cybersecurity.* Retrieved from https://www.sba.gov/content/introduction-cybersecurity

→ FloridaSBDC.org

Helping Businesses Grow & Succeed

Business Partner Engagement

When looking at your supply chain, it is important to know who your partners are, what cybersecurity solutions they deploy, and understand the information you share with them. Is all of that information exchange necessary? Any information that is shared should have appropriate precautions to ensure that the data remains safe. Those partners should also expect the same from you.

Having the appropriate cybersecurity planning could impact your ability to secure contracts with some companies or the military. With the rise of cybersecurity, it is becoming a contractual issue as a precondition of business. The vulnerabilities of a network of companies are far too great to risk for all the companies engaged in the transaction. Just as you are partners in the development of a product, you are also partners to ensure that critical company information is secure.

Looking Ahead

Supply chains traditionally focus on efficiency, predictability, and the physical security of goods in transit. However, small businesses that look to their supply chain as a competitive advantage must also give the same attention to the complexities of cybersecurity. The stakes are too high to ignore. A strong solution must include data security, and partners should work together to ensure they identify the weakest link and take appropriate steps to address it. With cybercriminals operating at the speed of light, small businesses must take appropriate steps to secure their information. Once these steps are taken, let's get back to business.

Recommendations:

- ☐ Build cybersecurity procedures in concert with business partners so that they have appropriate protections in place for your shared information.
- ☐ Consider cybersecurity as part of your contractual agreement with business partners and conduct regular risk assessments.
- ☐ Define requirements for data security and ensure that information is secured in all areas it is transmitted.
- ☐ Provide training for your employees and for the employees in the supply chain to ensure that staff takes steps minimize risk to exposing your company to hacking.
- ☐ The U.S. Chamber of Commerce urges business of all sizes to use the NIST Cybersecurity Framework[2] to manage their enterprise and third-party supplier risk.

2. National Institute of Standards and Technology. (February 12, 2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf