MARCH 2019

SUPPLY CHAIN SECURITY FOR SMALL AND MEDIUM-SIZED ORGANIZATIONS

ITSAP.00.070

SUPPLY CHAIN SECURITY

As an organization owner, have you ever paused to think about the kind of information you share with your supply chain? Do you know how suppliers are handling your and your client's information or where this information is saved? It's in your best interest to ask these and other questions to keep your organization secure. Like large organizations, small and medium-sized organizations are vulnerable to cyber attacks because they have a lot of sensitive information that attracts threat actors. Cyber attacks are not only costly to address, but can put your organization at risk.

A supply chain is the critical link formed between your organization and other organizations that help you serve your customers. Whether you own a flower shop or an advertising agency, the success of your organization depends on the quality and security of your supply chains.

WHY IS YOUR SUPPLY CHAIN AT RISK?

If you run a small or medium organization, you may feel like your organization is not a target to threat actors, but it is. According to Innovation, Science and Economic Development Canada, here are over 1.14 million small and medium-sized organizations in Canada. These organizations hold a lot of information. Therefore, it makes sense that your organization is an attractive target to cyber threat actors. Your supply chain can be targeted by threat actors for any of the following reasons:

- Your organization collects personal information from clients (e.g. name, address, phone number, email address, birthday).
- Your organization has trade secrets or other intellectual property.
- Your competitors want to know who are your clients.
- Your organization uses Point of Sale systems for payment information that holds credit card and client information.
- You're using vulnerable software or hardware.
- You're potentially connected, via your supply chain, to data or systems of interest to a threat actor.

Remember: even if your organization has top-notch security, a vulnerable partner in your supply chain is a risk to everyone in the chain.

HOW CAN YOU BUY SECURELY AND REDUCE RISK?

The first step in securing any supply chain is examining it for weaknesses. You may find vulnerabilities in your IT equipment and devices. Or you may find that some vulnerabilities are in other aspects of your supply chain, such as access controls (to physical premises or systems), transportation, and product sourcing. When evaluating your supply chain, start with some of the following considerations:

- Be aware that tampering and the use of unauthorised replacement parts can occur when electronic equipment is serviced or repaired.
- Ensure only trusted personnel have access to sensitive data (e.g. company secrets, financial information, personal information).
- Understand what needs to be protected (e.g. organization assets, sensitive information).
- Take the time to evaluate the kind of information you share with your suppliers and contractors.
- Request and assess the supplier's security plan of the facility if you intend to store sensitive information or devices off-site.
- Assess contract personnel who will work with sensitive information.

IT SECURITY CONCERNS

When it comes to supply chain concerns, you should work with your service providers to address them. Your service providers can be the firm hosting your online store or the IT service team you use to maintain company equipment.

Sample questions include:

- How do you protect customer data?
- How is the data encrypted?
- Where will any customer information I share be stored (in the cloud, onsite, on a PC)
- How long do you keep the information I provide you?
- How do you destroy shared data?
- Do you share information with any third-party contractors?
- How are your network and devices secured against attacks?

You should also have easily understandable processes and plans in place to help prevent security issues.

Sample processes include:

- Re-evaluating contractors and suppliers continually to ensure they still meet your security requirements.
- Evolving your supply chain security as your organization changes.
- Maintaining open lines of communication with suppliers.
- Adding contracting clauses to address basic supply chain risks when contracting for products and services that may impact your infrastructure or data.

WHAT DOES IT ALL MEAN?

A chain is only as strong as its weakest link. IT security and physical security should be a part of your organization operations. You should verify that what you buy and whom you buy it from is trusted and can be secured. When you take the time to understand and secure your supply chain, you're reducing the possibility of sensitive information falling into the hands of threat actors. In turn, customers will feel more comfortable engaging with your organization because they know you have taken steps to secure their information.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**