Cyber Liability

Reducing Supply Chain Cyber Exposure

Cyberattacks on global supply chains can cause irreparable harm to an organization's operational, financial and reputational wellness. These incidents can occur even if your organization is practicing proper cybersecurity methods. Instead of attacking your organization directly, these cybercriminals take advantage of vulnerable suppliers or vendors in your organization's supply chain to wreak havoc on key operations and compromise essential data.

Supply chain risk has increased dramatically in the last decade, as the internet has become a necessary element of various business operations. What's more, third-party breaches can be costly, increasing the average cost of a data breach by $207,411. Still, research shows this risk is largely being overlooked.

While it's not possible to totally eliminate supply chain risk, there are several steps your organization can take to reduce your supply chain exposure. Review the following guidance to understand what factors increase your organization's supply chain risk, how to mitigate them and what to do if your supply chain is compromised.

Where Does Supply Chain Risk Come From?

Supply chain risk can stem from a variety of parties and practices within your organization, such as:

- Third-party services or vendors with access to information systems
- Poor information security practices by suppliers
- Compromised organizational software or hardware
- Software security vulnerabilities in supply chain management or among third-party vendors
- Inadequate third-party data storage measures

Every organization has at least two levels of suppliers. This includes directly contracted suppliers (Tier 1) and the companies that supply to them (Tier 2). Very few organizations review the risk of their Tier 2 suppliers, leaving them vulnerable to supply chain cyberattacks.

What's worse, supply chain risk can increase dramatically a few months into suppliers' contract terms and may only continue to increase throughout these contracts if such Tier 2 suppliers are not properly vetted for potential cyber exposure concerns.

What Factors Increase Supply Chain Risk?

A wide range of factors have the potential to elevate your organization's supply chain risks, including:

- Complacency or inability of your organization or its suppliers to monitor and assess cyber risk
- Any changes in your organization's cyber risk tolerance
- The increasing severity and frequency of cyberattacks
- The increasing sophistication and boldness of cybercriminals

In the event of a supply chain cyberattack, cybercriminals may attempt to overwhelm your organization's networks and servers to

disrupt normal business activities. They may also try to copy, rearrange or destroy vital company data. Whatever their intent, a cyberattack on your organization's supply chain can be costly and time-consuming.

Understanding Your Supply Chain Exposure

There are several ways in which your organization can review its supply chain cyber exposure. Consider the following best practices:

- Create a vendor inventory of all third parties and consultants with access to your organization's IT network or sensitive data.
- Use a cross-functional, legal, compliance and privacy team to assist your organization in assessing its supply chain risk.
- Communicate with your organization's vendors about their specific cyber risks and what measures they have in place to mitigate these exposures.
- Review the cybersecurity policies and procedures in place within your organization and its suppliers for effectiveness.
- Assess your organization's physical and online processes to determine potential gaps in cybersecurity.
- Identify critical systems, networks and information within your organization to better understand how this data could be compromised and what actions are necessary to protect such data.

Decreasing Supply Chain Risk

Fortunately, there are some steps that your organization can take to help decrease its supply chain cyber risk. Be sure to implement these precautions:

- Incorporate cyber risk management into vendor contracts. This can include requiring vendors to obtain cyber insurance, having them notify your organization after a cyber incident and establishing clear expectations regarding the destruction of data following the termination of your contracts.
- Minimize access that third parties have to your organization's data. Once a vendor or supplier has been chosen, work with them to address vulnerabilities and cybersecurity gaps.
- Monitor suppliers' compliance to supply chain risk management procedures. Consider adopting a "one strike and you're out" policy with suppliers that experience cyber incidents or fail to meet compliance guidelines.

How to Respond to a Compromised Supply Chain

In the event that your organization's supply chain becomes compromised or exploited by cybercriminals, follow these response measures to mitigate the damages and prevent future incidents:

- Mitigate first. This could include patching or upgrading software systems, disabling internet access, or moving applications behind firewalls.
- Contact your insurer immediately. Make sure to reach out to your insurer as soon as the incident occurs. Give them as much information as possible to help kickstart the claim process.
- Engage legal counsel. Consult your organization's trusted legal professionals for additional guidance on adopting an appropriate response to the incident—such as whether to contact law enforcement or inform stakeholders.
- Enlist forensic expertise. Have forensic experts work with your organization to investigate the incident. These experts can help identify the perpetrator(s), determine potential cybersecurity gaps that led to the incident and offer tips for preventing similar supply chain concerns going forward.

For additional risk management guidance and insurance solutions, contact Schauer Group today.
