iStock.com/Contributor

MANAGING CYBER RISK

The growing need for cybersecurity in supply chain management

Your suppliers are most at risk, and attacks will be costly

BY ALEXANDRA WRIGHT, JACKIE VERGNE AND KEN RAYNER, *Cyber Insurance Solutions Inc.*

Many companies and organizations are moving their practices online because of COVID-19 and the nationwide lockdown to prevent the spread of the novel coronavirus.

In addition, more people are working from home and connecting with others through technology. More than half (56%) of employees are using their personal computers during the pandemic as a consequence of their company's policy to work remotely, according to the Work-from-Home (WFH) Employee Cybersecurity Threat Index. Nearly 25% of employees working from home don't know what security protocols are in place on their device; more than one-in-four have frequent issues with spotty Wi-Fi, limiting antivirus efficacy.

The increased use of the digital space for work brings supply chain issues into the foreground.

Many individuals put their trust in supply chain companies, but those suppliers can be the most at risk. According to Symantec's latest *Internet Security Threat Report*, attacks on supply chain increased by 78% in 2018. A variety of reasons account for the increase in cyberattacks; many of them start with "multiple points of contact" — i.e. many different organizations, or sources of information, coming together to conduct effective supply chain management.

With the increase of online interaction, and in an effort to mitigate cyberattacks, many companies are shoring up their online infrastructure, increasing the use of firewalls, and bolstering their digital security. But perceiving supply chain security primarily as an IT problem may result in overlooked exposures. Supply chains have many seamless connections between vendors, suppliers, and enterprises. Each communicate important information and provide an area of weakness for external attack.

It's important for companies to introduce new technologies to improve consumer interface and automate administration. But that comes with a risk: For

> Many individuals put their trust in supply chain companies, but those suppliers can be the most at risk. According to Symantec's latest Internet Security Threat Report, attacks on supply chain increased by 78% in 2018.

cybercriminals, it's a new way to breach security and steal important information.

Supply chain cybersecurity must be looked at as a whole, because third-party contracts can be a way of entry into a supply chain system. Supply chain is only as strong as its digital weakest link; a breach in security can severely affect an organization. Supply chain cyberattacks are not just common, they are costly. In a survey conducted by independent organization Vanson Bourne, 66% of 1,300 surveyed IT professionals reported experiencing a software supply chain attack. Of those surveyed, 90% described significant financial costs, with the average being US$1.1 million.

Attacks on supply chains are becoming more complex; each time it happens, some aspect of the supply chain, including people and vendors, must be be assessed for their own digital risk.

According to Symantec's report, the reasons for the high increase in supply chain cyberattacks are two-fold: 1) infiltration through third-party suppliers; and 2) malicious malware is being integrated into larger software.

Third-party suppliers

Supply chains are highly vulnerable due to the fact that they are interconnected. This interconnectivity is essential to the business, but significantly increases the risk to a cyberattack. Hackers are not trying to penetrate firewalls so much as they are encrypting themselves in software used by one of the connected organizations.

Cyberattacks can happen against smaller software companies that have weaker cybersecurity. Vendors, suppliers, or the supplier's suppliers, may use this software, exposing the entire supply chain to an attack. Larger companies, including insurance companies, have fallen victim to the trap of not properly vetting

> Supply chain is only as strong as its digital weakest link; a breach in security can severely affect an organization.

and securing entry by suppliers. Changing a supply chain management system takes financial investment, time, and human resources. If not implemented properly, the resultant wasted labour, service redundancy, and missed deadlines may be costly.

In 2018, Ticketmaster, a ticket sales and distribution company, announced that public information had been hacked and consumer information stolen. The target was payment information from customers. They were hacked through a third-party supplier. The hacker community is well aware that the easiest way into a large company's security is through a smaller, weaker organization.

As the demand for online resources and supply chain becomes even more critical, the need for a strong and resilient cyber infrastructure becomes even more important.

The global supply chain

Many products have multiple parts that are manufactured globally. Companies that make, buy, sell, or trade the parts use outside software and hardware. Different parts are made by multiple companies, suppliers, contractors from across the globe, creating a scattered source of much-needed parts. Cyberattacks can be delivered through both the hardware and the software. A hacker can infiltrate software using a number of different methods.

It can be easily infected through software updates, replacing legitimate files with malware. If hackers are able to trick a user into sharing sign-in information at the developer stage, they can build a stronger attack, entering malware into the software before its even shipped to customers; this makes the malware even harder to find once it reaches the consumer.

One vulnerable point is open-sourced information, often used to develop software. Many open-source libraries and frameworks provide a strong foundation for new technologies at a better price. They can be essential for creating innovative technology while improving efficiencies, building on existing software and elements to create a technology solution. The downside is that these sources can be compromised. Embedded with malware, they create a higher risk for use.

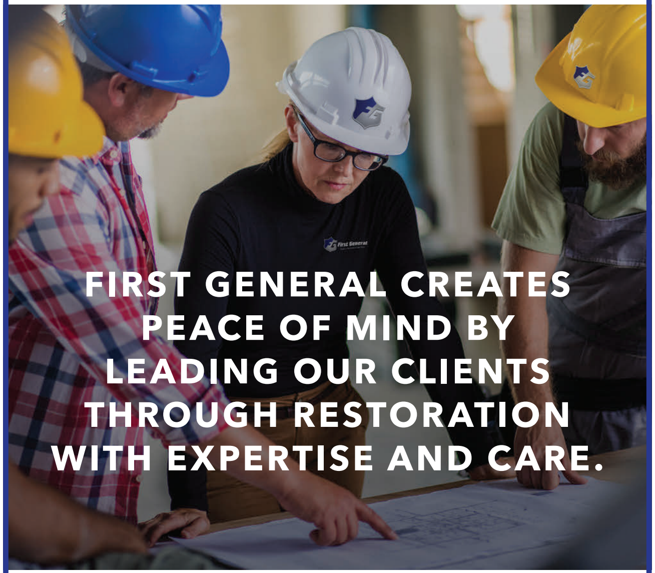
Supply chain software and technology interfaces — such as customer relationship management and enterprise resource planning — are often outsourced to other organizations to reduce infrastructure costs and create interoperability. This ties into the first issue mentioned above: Adding a third-party adds additional risk.

Outsourcing to other organizations can reduce costs, but it increases risk if those organizations don't have the correct cybersecurity processes in place. Hardware can be just as much at risk as software infiltrations. Counterfeiting, theft of intellectual property, and installing malicious parts can be a large market for those who are looking to make a profit.

Cyberattacks can go beyond software and into the hardware. Counterfeit parts are more common than most people think. The U.S. Department of Homeland Security released a report stating that 34,143 counterfeit parts were seized in 2017, with 12% of the products being safety and security-related products. Each purchased device and downloadable application needs to be vetted and examined for potential security risks to reduce the risk for malicious products to enter a supply chain.

Protecting supply chain

Organizations should emphasize cyber resilience to maximize their business opportunities while mitigating cyber risk. When an organization has a breach in their cybersecurity, it's not only


FIRST GENERAL CREATES PEACE OF MIND BY LEADING OUR CLIENTS THROUGH RESTORATION WITH EXPERTISE AND CARE.

> Supply chains are highly vulnerable due to the fact that they are interconnected. This interconnectivity is essential to the business but significantly increases the risk to a cyberattack.

costly to fix, it erodes consumer trust.

You can reduce vulnerabilities in supply chain digital security in many ways. One to ensure each software supplier and third-party vendor is secure. Suppliers must be screened; their security risk should be assessed before working with supply chain organizations. High standards must be developed and enforced for both third-party and for employees. Employee education and risk assessment is essential. Each employee must understand their own risk and the best way to mitigate cyberattacks, for their own safety and that of an organization.

Supply chain organizations and their third-party suppliers must use best practices, including a cyber risk assessment. To reduce risks of using open-source software, each component should be assessed. A security analysis helps to understand the risk of use and highlight vulnerabilities.

A secure supply chain is vital since individuals and organizations are moving their practices online, ordering more stock and sharing information. It's costly to ignore the risk of cybersecurity. The strongest supply chain organizations have not only minimized their cyber risk, but they have promoted this fact to gain trust from their various stakeholders.

An important contract term for insurers is "supplier obligation management." Insurers must take appropriate steps to manage their supply chains by requiring that each supplier describe, and guarantee, the cyber health of their organization. In other words, suppliers must demonstrate their "percentage of cyber preparedness" as a condition of becoming a supplier. cu

Alexandra Wright and Jackie Vergne are consultants and Ken Rayner is vice president with Cyber Insurance Solutions Inc. and Cyberisk Chek Inc.