CYBALT

# Supply Chain Risk Management – Where and How to Start?

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

# Supply Chain Risk Management – Where and How to Start?

Events over the past few years have taught us in no uncertain terms how important supply chains are and how we take them for granted. In the pre-pandemic years, if we wanted something, we went to the store or online and bought it. Once purchased, we received our items over night or within a very few days. The laws of supply and demand seemed to be working quite well. Not anymore.

Today, when you go to buy something, almost anything, from a bicycle and electronic game to large purchases, such as an appliance or a car, you will most like encounter some type of supply chain disruption. Most people think backorders, unavailability, long wait times, and substitutions are the result of poor planning, natural disasters, chip shortages, shipping delays, labor shortages, and more. And they will be correct. But there is another, often overlooked but critically important risk — security.

**The Sleeping Giant**

In the world of supply and demand, where everyone expects faster delivery and product shipping, the supply chain is being driven by technologies that have evolved over the years. The technology worked well in the background and supply chains continued to flow normally. Everything worked as it should.

However, the same technologies that make supply chains faster and more effective also threaten their cybersecurity. Supply chain security is the sleeping giant, forgotten, overlooked, and underestimated. On the contrary, supply chain cybersecurity should be a high priority for organizations, as a breach within the system can damage or disrupt operations. Vulnerabilities within a supply chain can lead to unnecessary costs, inefficient delivery schedules, and intellectual property loss. The economic ramifications can grow exponentially the more complicated the supply chain.

Supply chains have touchpoints with manufacturers, suppliers, and other service providers around every corner. Every company involved in the supply chain must understand the risks and respond to them. To mitigate this critical problem, companies need to consider cybersecurity while designing a new supply chain or redesigning an existing one. Information Technology Decision Makers (ITDMs) must start thinking about the supply chain cyber-attack as a part of their risk management plan.

Supply chain cyber attacks are on the rise, and hackers are targeting every company in the supply chain ecosystem, from the end-user organization to the software providers to the suppliers. Remember, a chain is only as strong as its weakest link. This applies to supply chains as well.

**Short-sighted Investments**

It has been observed that throughout the COVID pandemic, companies heavily invested in their IT/OT infrastructure to ease the growing pressures on the supply chain. While these investments may be targeted at improving logistics, they are still short-sighted. Very often, ITDMs only considered the physical. They did not consider investing in holistic cyber management programs, which has left vast attack supply chain link surfaces open and vulnerable to attackers.

Although there is a favorable trend in supply chain management aimed at reducing cyber security risk, there is still much work to be done. While exact figures are difficult to come by, the tendency is undeniable.

**Supply Chain Cybersecurity Best Practices**

Just as organizations go to great lengths to keep their networks locked up tight, every organization should employ a few best practices to mitigate supply chain cybersecurity threats.

**1. Identifying the threat landscape**

*"A mistake that is being repeated is not a mistake. It's a choice."*

Despite clear evidence pointing to the severity of the supply chain cybersecurity threat, some industry leaders aren't ready to face that reality even if they understand the techniques needed to build broad supply chain resiliency.

The first step is to conduct a cybersecurity maturity assessment on technologies deployed sligning to the industry-standard frameworks like ISO 28000:2007 and NIST Cybersecurity Framework (CSF) 1.1. Management should make a roadmap working in the risks observations of the assessment reports.

**2. Implementing heterogeneous supply chain security strategy**

Hackers want to attack the supply chain with different goals in mind — from ransom to sabotage to the theft of intellectual property. It's an extensive area that includes everything from physical threats to cyber threats, from protecting transactions to protecting systems, and from mitigating risk with parties in the immediate business network to mitigating risk derived from third, fourth, and "n" party relationships.

With the growing frequency and ferocity of cyberattacks, supply chain leaders need to enhance the coordination between the IT security team, risk management team, and supply chain team.

**3. Digitization and remodelling**

Relying on old-school paperwork, phone, fax, and email communications for corporate transactions creates a slew of modern-day data security concerns. First (and last), it is vitally critical to digitize specific manual procedures. Conduct a feasibility study into ways you can quickly transition from manual, paper-based processes to secure digital systems that provide security, reliability, and governance. The benefits of converting the company's working paradigm from manual to digital include encryption, tokenization, data loss prevention, file access monitoring and alerting, and security awareness and training for teams and partners.

**4. Evaluate supplier risk**

The use of third parties such as agents, distributors, consultants, channel partners, counterparties, and customers presents a host of legal, regulatory, and reputational risks to an organization.

ITDMs and the security gate keepers must ensure that third parties comply with applicable laws and regulations like anti-bribery and anti-corruption, know your customer (KYC) rules for money laundering and terrorist financing, and the organization's internal policies and procedures. As businesses grow their supply chain, the need for a robust and sustainable third-party risk management (TPRM) program will be more critical than ever before.

**5. Incident response planning and orchestration**

We all know the phrase, the best offense is a strong defense. That's why you need to proactively prepare for a breach, shut down, or disruption, and have a robust incident response plan in place. Practiced, tested, and efficiently executed response plans and remediation prevents revenue loss, reputation damage, and partner and customer churn. Intelligence and programs provide metrics and information your organization and partners can use to make decisions as how to prevent attacks or incidents from occurring again.

**Every Touchpoint is a Vulnerability**

All tech-enabled corporate processes and capacities are vulnerable to cyberattacks. The supply chain stands out as being extremely vulnerable in terms of the number of handoffs. Every link in the chain, every "hand off," is a new risk. From the raw materials to the finished product and service, and everything in between, including labor, the more links you have, the more vulnerable you are. Every link along the extended, end-to-end supply chain — plan, source, make, deliver, and customer support — are possible touchpoints for cybersecurity attacks. While automation and digitization of processes and goods have many advantages, together they only assure that the supply chain cyber risk frontier continues to grow.