It’s now or never to get ahead of supply chain cyber risk

Addressing cybersecurity risk and building a resilient supply chain should be a top agenda item for nations and corporations.

BinaryCore | KEARNEY

It’s now or never to get ahead of supply chain cyber risk

Addressing cybersecurity risk and building a resilient supply chain should be a top agenda item for nations and corporations.

Our ever-evolving dependence on increasingly complex supply chains is a growing concern for organizations when it comes to their ability to build and deliver. The COVID-19 pandemic and ongoing geopolitical tensions, such as the war in Ukraine and rising concerns over the security of Taiwan and its supply base, are contributing to rising costs and shortages of supplies such as electronic chips for many manufacturers. This situation serves to demonstrate the fragile nature of the supply chain, and more crucially its criticality at a national security and welfare level.

This fragile balance makes the global supply chain a perfect target for not only state-sponsored cyberattacks but also a broader and more sweeping wave of cybercrime (estimated to have a global market value of $11 trillion by 2025). Now with cyberattack tools becoming a commodity, with the cost to execute as low as just a few dollars, and relatively low risk of prosecution, a new generation of criminals has emerged. The attacks we are seeing now are targeted, complex, and in many cases perpetrated over an extended period to achieve maximum impact, with the likes of APT, ransomware, and malware. The fragility of supply chains has been demonstrated, as has the willingness of companies to pay ransom. This has set the stage for more supply chain infiltration and disruption in the coming years.

A recent study showed that total supply chain disruptions in just US and European companies reached around $4 trillion in 2020. The 2019 BCI supply chain resilience report highlighted that around a quarter of supply chain disruptions were caused by cyberattacks and data breaches. Based on these data points and approximations, we can estimate that cybersecurity-related disruptions in the supply chain have cost businesses $1 trillion in the US and Europe alone.

Tackling cybersecurity risk and building resilience in supply chains should be a top priority for nations and corporations, and the question is no longer if an attack is coming, but what is already under attack and when the impact is going to present itself.

> We estimate that cybersecurity-related disruptions in supply chain have cost businesses $1 trillion in the US and Europe alone.

Third parties are at the core of cybersecurity risks in supply chains

In 2020, the US government and global organizations were targeted (primarily) via SolarWinds' systems hosting a malware that granted perpetrator access to critical data systems. Despite many of these organizations having implemented advanced cybersecurity capabilities (for example, the US military), the attackers were able to exploit a weak link in the chain. With organizations increasingly targeted through their supply chain, third-party risk is a serious threat to stability. In recent years, it is estimated that around 50 percent of cyberattacks came from third parties, with negative effects on customer churn reaching 20 percent. Several factors account for the increased cyber risk in third-party interactions:

Increased digitalization and system complexity
As companies digitalize, they're increasingly interconnecting their systems with other companies across their value chain that could be sources of cybervulnerabilities. These systems are managed by a multitude of vendors with varied accountabilities, cybertools, and skills. They use hardware and software from a large cross-section of providers, which in turn creates a complex and opaque ecosystem to manage. Unfortunately, many solutions providers disregard, or are unaware of, the software supply chain risks they represent to their customers, and they have not vetted the organizations within their supply chains they have connected with.

Additionally, as organizations accelerate their go-to-market strategies to gain first-mover competitive advantage, it is at the expense of robust cybersecurity protections and testing, leaving their solutions ripe for exploitation further down the line. A study from Sonatype showed that next-generation software supply chain attacks increased by 650 percent in 2021. The challenge of detecting supply chain vulnerabilities further increases the chances of zero-day attacks and attack spillover. In industries where IT and OT are converging, this is an area for growing concern due to the potential of core operations being disrupted. Cyberincidents are no longer limited to traditional information technology (IT) systems; operations technology (OT) systems are equally vulnerable and a growing target. In fact, cyberattacks on industrial control systems have risen by 116 percent since 2016.

Excessive and unchecked administrative privileges
With the war for cyber talent intensifying, the challenge of attracting and retaining skilled security and system administration staff is great. This talent challenge has resulted in an increase in enterprises relying on the outsourcing of systems management. One consequence of this dilemma is that third-party organizations are often given more system administration privileges than is actually necessary or appropriate. As time passes, these privileges are rarely revoked, even as the individual moves into different roles or out of the organization entirely. Many organizations also grant senior leaders access privileges beyond their daily need. This open access approach without proper vigilance increases the cyber risk threat potential. Hackers, well aware of such privilege governance issues, seek to exploit these prime entry points for their attacks.

Fragmented standards and regulation
While most countries have developed cyber standards and regulations at a national level, there is no global harmonization, resulting in major challenges when it comes to robust legal enforcement on the international stage. As a result, companies operating in countries with a weak regulatory framework, and that are part of a global supply chain ecosystem, become easy targets for cybercriminals, creating a perfect storm in which to shelter the attackers. This situation is true for most global manufacturing enterprises.

Compliance mindset
Designing a cybersecurity strategy from a compliance perspective, is not always an ideal long-term solution. While it may protect the organization from a regulatory perspective, it limits the opportunity to adopt a proactive footing and anticipate and plan for future disruptions. If regulations are unable to evolve at the same pace as the cyberadversaries, and enterprises rely on government guidance, then enterprises can quickly find themselves vulnerable. The "compliance mindset" as the guide to sufficient protection can be a dominant force within a company hierarchy but can hinder proactive actions and introduce significant risk. Regulations should be viewed as the absolute minimum, then the organization must evaluate its risk profile and tolerance and determine what more it should do. When an event occurs and is made public, two questions will arise: When did it discover the compromise? Did it take all the precautions of a prudent organization? The answer to these two questions can have great financial consequences.

For companies with a reactive risk management strategy, and lacking in appropriate resources, the challenges outlined above pose a very real threat that is too great to be ignored.

> With organizations increasingly targeted through their supply chain, third-party risk is a serious threat to stability.

The winning formula: a value-at-risk approach to cybersecurity strategy

Tackling supply chain risks is no easy task, but the companies that are successfully navigating the choppy cyber seas have security firmly pinned to the top of the leadership agenda and are developing strategies and action plans that are deliberate and focused on securing their "value-at-risk."

Conduct regular—and comprehensive—"value-at-risk" assessments
Identify the critical assets your company must protect and determine the level of risk you are willing to accept. All organizations have data, information, and systems that are more valuable than others for various reasons—from protecting intellectual capital to maintaining safety and safeguarding customer information. A formal review of assets to identify the most important ones is essential to determining the acceptable levels of risk and creating the security controls necessary to protect them. The assessment also includes third-party providers, because service providers often have access to the assets of companies they work with. A cybercriminal who attacks one of these service providers may be able to access other companies' assets as well. This vulnerability is magnified by the fact that companies often outsource central components of their businesses and most have very little understanding about the number of vendors that have access to their sensitive data.

Design disciplined vendor risk management capabilities
Our research indicates that less than one-fourth of companies are aware of the data-sharing that occurs in their vendor/partner relationships. Design and implementation of a robust vendor security management strategy and processes are essential. Vendors undertake a mandatory security assessment that ensures secure SLAs are adopted. It is crucial to conduct regular risk assessments as part of vendor performance reviews and take extra care when offboarding vendors to ensure that all access is revoked. It is important to note that these cybercontrols should be implemented for all service providers that have access to sensitive data—not just tech providers. Controls should be based on a specific provider's level of access rather than the type of provider.

However, enforcing such security requirements is not always easy when dealing with global suppliers, particularly those with real market strength. Leveraging industry associations can be helpful to balance the power of the partnership and encourage the required security guarantees. While cyberattacks are global in nature, there are differences in the preparedness of countries and their capacity to respond. Given this variation in the levels of cybersecurity among countries that are potential destinations for outsourced and offshore operations, companies seeking to outsource must pay attention to the cyber risk profile of countries in which their service providers are located, in addition to assessing the risk profile of the providers themselves. Kearney's Global Services Location Index (GSLI) includes a digital resonance dimension that encompasses cybersecurity preparedness, response, awareness, and legislation.

Combining industry indices that rank countries based on their legal, technical, organizational, capacity building, and cooperation maturity, this benchmark can inform the crucial service provider cybersecurity threat assessment that all companies must now be conducting at a high level.

Elevate cyber risk reporting to board level

Cybersecurity should be immediately elevated to the board level with relevant, timely reports to leadership at each level. Develop weekly reports for leaders so they are aware and prepared to act as soon as needed. As the firm develops contingency plans for business continuity, it is essential to plan for any unwarranted cyber threats and how to recover. From a customer management perspective, transparency and communication are fundamental to mitigating attack impact. Not only do they help to build trust and confidence in doing business with the organization, but they can also help reduce, or stop entirely, attack spread. Successful companies frequently conduct regular incident readiness exercises to test and reinforce their communication response and deployment drill. The board-level reporting can further support alignment on key messages for the customers and shareholders.

Drive leadership accountability with clarified lines of defense

Between 70 and 80 percent of cybersecurity attacks succeed due to people, process, and organizational weakness or blind spots. Through a collaborative approach to structuring the security organization using accountability, ownership, and responsibility as the cornerstone, leaders have managed to create strong cyberawareness and response cultures. If your firm does not have an assigned security leader, there is likely no clear accountability for recovering from an attack. Clarify the lines of defense and decision-making rights in case of a cyberattack. Clarify roles across your IT, business continuity, and security teams to ensure single accountability for managing security requirements and mitigating risks. Leadership accountability also helps employees dealing with third parties to act more cautiously, while phishing and social engineering attacks have a much lower success likelihood. Senior executive endorsement and monitoring of supply chain risk management also helps secure additional required resources and talent, but it also sends a clear signal of the importance of this topic as a key priority to the rest of the organization—and beyond. It is also important to plan ahead. Review and modify your financial forecasts to consider realistic worst-case scenarios across your business, including the possibility of cyberattacks. Identify the leading indicators of online exposure with more frequent vulnerability tests across your entire cyberlandscape and trigger immediate actions for any early signs of an intrusion.

From a core capabilities perspective, and in a market context where the war for cyber talent has never been so competitive, attracting, developing, and retaining skilled security employees is key to either perform important tasks within the organization to help minimize risks, or, with increasing importance, manage the tasks that have to be outsourced and that therefore increase the risk exposure of the organization.

Design and implement technology solutions that help alleviate vulnerabilities

Security by design and continuous patch management are two practices that have advanced companies operating with robust and secured technological products and architecture, with some of these organizations going a step further still by implementing zero trust architectures to limit the spread of malware. They also implement strict technology security compliance checklists and vendor SLAs, monitor their applications closely, and account for mitigation measures in cases of undiscovered noncompliance. This becomes even more relevant in the context of software supply chain risk, and companies should carefully assess how their vendors can and will mitigate that risk.

Rebuilding the technology landscape based on "industrialization with localization" concepts helps develop a template-based architecture that allows for standardization of cybersecurity controls and site-specific localization. A future-proof architecture design is vital to effective control as companies add more connected devices that share third-party data. Develop an "existing-first" approach to cyberinvestments to extract the most value from the technology investments with the least amount of risk.

> Between 70 and 80 percent of cybersecurity attacks succeed due to people, process, and organizational weakness or blind spots.

Public–private sector collaboration is reshaping resilient supply chains

Increasingly we are seeing the rise of private–public sector collaboration, especially given the ability for government agencies to identify and classify companies considered as critical national infrastructure and support their efforts in protecting critical assets across the supply chain. The breadth of support available can include cybersecurity investment and research incentives, as well as many other options. One example of this collaboration is the Cybersecurity Supply Chain Risk Management project initiated by NIST, which helps organizations to manage the increasing risk of supply chain compromise related to cybersecurity, whether intentional or unintentional.

For this collaboration to be successful, regular and robust cyber maturity assessments of these vital organizations must be conducted to assess consistent improvements in their stance to cyber risk. Other levers at the disposal of government to reinforce the existing regulatory framework include:

1. Ensuring executives and boards are directly accountable for cyber risk and take appropriate measures to mitigate it
2. Legislating that foreign companies that wish to operate from their shores comply with local regulations
3. Increasing the coverage of OT and IoT security

By combining these three regulatory levers with enhanced cross-border collaboration, a powerful cybersecurity counter platform starts to take shape. To be successful, this cross-border collaboration must be underpinned by best practice sharing, information and intelligence sharing, immersion programs, capabilities reinforcement and investment, and sponsorship of cybersecurity-related international associations. With cyberadvanced countries taking the lead and fostering collaboration networks with less-mature cybernations, global measures and standards will be more rapidly adopted and enforced to protect businesses, and by extension the global supply chain.

While nations in the past have passed and implemented nationwide laws to protect their critical infrastructure, our recent supply chain resilience assessments across industries reveal that cybersecurity continues to fall well short of the standards required, given continually evolving disruptive market conditions when it comes to developing a robust and proactive cyber strategy, as well as adequately implementing and integrating effective governance and processes. In the report, we have shown that supplier diversity is one of the most underperforming dimensions of the compass that needs to be addressed very soon.

With recent events continuing to highlight global supply chain weaknesses and ongoing vulnerabilities, alarm bells are ringing louder than ever for nations and companies that do not currently have this topic at the top of the leadership agenda. Cybersecurity is now a business problem—the defense strategy should be underpinned with global best practices to ensure rigor and legitimacy, linked to the organization's value at risk. Our experience with a variety of companies indicates that the likelihood of avoiding and effectively managing an exposure surges when the cyber defense plan is integrated with both the digital vision and the broader supply chain resilience and business contingency strategy.

Note: Kearney and BinaryCore (Kearney's deep-tech solutions business) work collaboratively with global organizations to determine your status quo, quantify your exposure, and develop and implement appropriate and robust risk management strategies to address your supply chain risks. Read our latest thinking with the World Economic Forum on cyber resilience.

The authors

Ronny Schubhart

Senior Cyber Engineer,
BinaryCore, Munich
ronny.schubhart@binarycore.com

Michael Roemer

Co-Founder, BinaryCore, and
Partner, Kearney, Munich
michael.roemer@binarycore.com

Vidisha Suman

Partner, Kearney, San Francisco
vidisha.suman@kearney.com

Dieter Gerdemann

CEO, BinaryCore, and Partner,
Kearney, Munich
dieter.gerdemann@binarycore.com

Guy Ngambeket

Consultant, Kearney, Doha
guy.ngambeket@kearney.com

Clif Triplett

Senior Advisor, Kearney,
Washington, D.C.
clif.triplett@kearney.com

About BinaryCore

BinaryCore was born from a need to tackle complex technology challenges businesses face in an era when realizing the full value potential of software engineering and cloud usage will clearly distinguish the leaders from the laggards. But addressing these challenges requires radical step change—a willingness to unlearn what went before, an openness to new possibilities and partnerships, and the confidence to make bold decisions and rewrite the rules.

With deep technology expertise, powerful proprietary software, a sharp focus on the numbers, and a clear set of rules, we'll guide you every step of the way to transform your technology and talent set and put in place the infrastructure and teams needed to set you up for long-term success.

binarycore.com

About Kearney

As a global consulting partnership in more than 40 countries, our people make us who we are. We're individuals who take as much joy from those we work with as the work itself. Driven to be the difference between a big idea and making it happen, we help our clients break through.

kearney.com

BinaryCore | KEARNEY