Modernizing Supply Chain Risk Management

February 2023

www.RMCGlobal.com

This paper is designed to provide analysis of relevant, publicly available information regarding the current supply chain threat landscape and its impact on organizations worldwide. This product provides a foundational perspective on the evolution of supply chain risk based on the analysis of current trends and analyst expertise and is not intended to provide a detailed blueprint for establishing a holistic SCRM program.

Evolution of supply chains and the rise of a new threat

Global supply chains are as fragile and vulnerable as ever. As new competitors and innovative technologies constantly reshape the corporate landscape, companies are increasingly looking to their supply chains to provide a competitive advantage. Historically, companies have optimized their supply chains for responsiveness and efficiency to deliver products to their customers. In recent years, as pandemic disruptions and malicious threats threw evolving global supply chains into disarray, some companies have come to appreciate the need for both security and resiliency. However, as supply chains begin their slow march towards a new normal, companies are falling back on old habits, failing to appreciate security and resiliency as design considerations equally important to responsiveness and efficiency.

As global supply chains evolve to include an ever-increasing array of technology and outsourced business processing in addition to the widgets and commodities of yesteryear, industry's myopic focus on supply chain responsiveness and efficiency overlooks potentially existential threats. While all external relationships require a level of inherent trust, these new links in the supply chain require unprecedented access into the inner confines of an organization, drastically increasing the risk exposure of the modern supply chain.

Furthermore, rapid digitization and its resultant proliferation of data has magnified the risks posed by insecure and vulnerable supply chains. The interconnectedness of today's supply chain exponentially increases the surface area exposed to the outside world that companies must protect from compromise. Similarly, the increasing reliance on data to optimize business operations introduces more opportunities for its compromise. These opportunities multiply as companies share data further into the supply chain to derive better insights and achieve greater visibility.

As supply chains evolve to include unprecedented links between companies, malicious threat actors seek to exploit novel entry points to attack supply chains and cause widespread disruption. Supply chains present two enticing opportunities to threat actors: (1) Exploit the inherent trust in the supply chain by using vulnerable suppliers to target and compromise hard targets and (2) Efficiently compromise many organizations from a central link in the supply chain. The opportunistic attacks are especially dangerous, since their indiscriminate nature can result in painful impacts for organizations large and small.

The need for a sea change in SCRM

To effectively secure modern supply chains from these rapidly evolving threats, organizations must expand their focus from supply chain responsiveness and efficiency to include supply chain security and resiliency. Supply chain risk management (SCRM) programs must constantly evolve to keep pace with the changing threat landscape, ensuring that each third-party down the supply chains are sufficiently resilient and secure.

Modern SCRM programs must be threat-informed, efficient, and dynamic. The unfair reality is that security professionals must account for all vulnerabilities and the threats only need to find one. Companies that tailor supply chain security efforts to current threats by developing threat-informed SCRM programs, level the playing field greatly increasing their ability to defend against supply chain attacks. Effective SCRM programs integrate with existing business processes and leverage technology to direct due diligence efforts toward areas with the greatest potential to defend against the threats that are actively targeting relevant vulnerabilities and risks. Periodic and one-time due diligence efforts alone are insufficient to confront these dynamic threats. It is crucial that SCRM programs have mechanisms to identify shifts in the threat landscape and the impact to their supply chain security posture so companies can proactively adjust due diligence practices to remain vigilant throughout the supply chain.

Modernizing your SCRM program

Effective SCRM modernization initiatives must start with an objective assessment of the current maturity of the program. This assessment needs to define business objectives, decompose current processes, clearly define risk appetite, and critically examine the strategic goals of the organization. Only with the understanding from that objective assessment can a company begin to design and integrate modern processes and cutting-edge technologies as well as upskill their workforce to meet today's dynamic threat environment.

SCRM program considerations

There is no one-size-fits-all SCRM program that companies can simply plug in and deploy. Companies must methodically tailor their SCRM programs for their specific operating context. Even though SCRM programs are unique to each organization, there are several guiding questions that executives should consider to ensure modernization efforts are optimized for the company context.

How does third-party classification influence risk assessment scoping?

Each third-party (e.g., a vendor) presents a different risk profile to the supply chain and the outsourcing company. Effective third-party classification accounts for the business risk of the outsourced activity and the company's risk appetite in that area. Classification based on these factors creates the foundation necessary to properly scope risk assessment and monitoring activities. Creating a process that uses scarce resources to not only focus on the riskiest third parties, but also the riskiest aspect of the outsourced relationship maximizes return on investment.

How does the third-party support the business?

What assets / access will the third-party need?

What is the third-party's historical security posture?

Considerations when classifying third-parties

What level of due diligence is sufficient to understand the risk in my supply chain?

The third-party classification process should determine the depth and type of due diligence performed. The inherent risk identified in the classification process informs the level of due diligence needed, which could be simple contractual obligations or more intrusive regular onsite audits of the control environment. It is equally important to consider the type of due diligence performed. Based on the third-party's role and importance in your supply chain, you can focus due diligence in the areas with greatest potential impact while taking a less resource-intensive approach in areas of minimal relative benefit.

How can my SCRM program keep pace with the dynamic threat environment?

The threat landscape is constantly changing. For SCRM programs to keep pace with this rate of change, a hybrid assessment approach is called for. A hybrid assessment approach combines the depth of point-in-time assessments with the broad dynamic scope of continuous monitoring, resulting in a holistic illumination of risk throughout the supply chain. For this approach to be effective, continuous monitoring must be requirements-based. Put simply, you should never monitor for a scenario in which your organization cannot or will not act on. Overly broad monitoring of complex supply chains quickly turns valuable information into alert fatigue, burying critical insights in the noise.

What makes supply chain risk insights actionable for my organization?

Actionable insights start with asking the right questions. Industry compliance standards, while a great starting point, seek to cover all possible situations and are not tailored to your unique operating environment. Asking the right questions will arm your SCRM team with the information they need to better inform decision-making in the outsourcing process. When risk insights are made, there must be an existing structure that ensures follow through and proper tracking of issues. More than anything else, empower your team to prioritize risk over compliance. Asking a supplier to implement a control that checks a box but does not reduce your risk exposure is not only a waste of time and resources but can even degrade your credibility and reduce cooperation.

Let's talk about your SCRM needs today – email us at sales@rmcglobal.com