Building Supply Chain Resilience Amid Increasing Cyber Concerns

STRATEGICALLY ASSESS AND MITIGATE RISKS TO BETTER PROTECT YOUR ORGANIZATION

Supply chain risks come from a wide range of sources. Cyber threats, including ransomware, malware, and other potential disruptions from bad actors with criminal intent, are numerous and varied. Supply chain interruptions can also come from changing climate conditions, extreme weather, and natural disasters. Political issues—including war, threats from nation-state adversaries, global regulations, and corporate and industry environmental policies—can all further threaten the stability of your supply chain. However, many of these factors can be mitigated by a robust, comprehensive risk management strategy that includes proactive cybersecurity.

As cybersecurity threats intensify, and evolving political issues add other potential challenges, organizations must develop greater resilience in their supply chains. The first step in building resilience is understanding prospective threats and the impact they could have on your supply chain. In the face of such a diverse threat landscape, boosting cybersecurity will reduce risk throughout the entire supply chain.

RECOGNIZING CYBER RISKS

An organization's ability to carry out its core mission is either directly or indirectly supported and enabled by all the businesses in its supply chain. As a result, not only do you need to be cognizant of the risks and challenges facing your own organization, but you need to ensure you can trust the resilience of all the businesses at every stage of your supply chain as well.

Priority one in supply chain risk mitigation must be making sure your own corporate network and systems are protected from the myriad of cyber risks and potential scenarios that could compromise your data or disrupt your business continuity, whether from external actors or from elements within your supply chain.

The biggest challenge is gaining a comprehensive understanding of how realistic the threats are and how potential supply chain vulnerabilities could affect operations, business continuity, supplier-to-customer relations, and more. For example, if a cyber threat causes a critical network to shut down, or connectivity is lost due to a cyberattack on your power supplier, how will you maintain continuity in your operations? What are the cost implications of this unplanned downtime? In industries like healthcare, energy, and water, would a supply chain disruption have a negative impact on the public? These issues highlight why, amid ever-increasing cyber risks, a wider strategic approach to building resilience throughout your entire supply chain becomes so crucial.

Guidehouse

INCREASING AWARENESS

Lack of awareness of key risks and their potential impact leaves organizations exposed and vulnerable to a wide range of cyber and other kinds of threats. The following steps can help guarantee that your organization's leadership is aware of risks and prepared for them:

- Assess the baseline threats and risks to your industry, suppliers.
- Develop an understanding of how threat actors may operate.
- Conduct thorough threat assessments and communicate the results to leaders and senior decision makers to ensure full awareness of the risks facing your supply chain.
- Illustrate to senior leadership how potential risks can affect your organization.
- Educate the leadership team on the strategic actions to take under various scenarios.

SETTING A STRATEGY TO MITIGATE RISK AND BUILD RESILIENCE

Addressing risk and developing a resilient supply chain requires a holistic strategy, aligning people, processes, technology, and external relationships. This is especially important when it comes to the extremely complex and volatile cyber threat landscape.

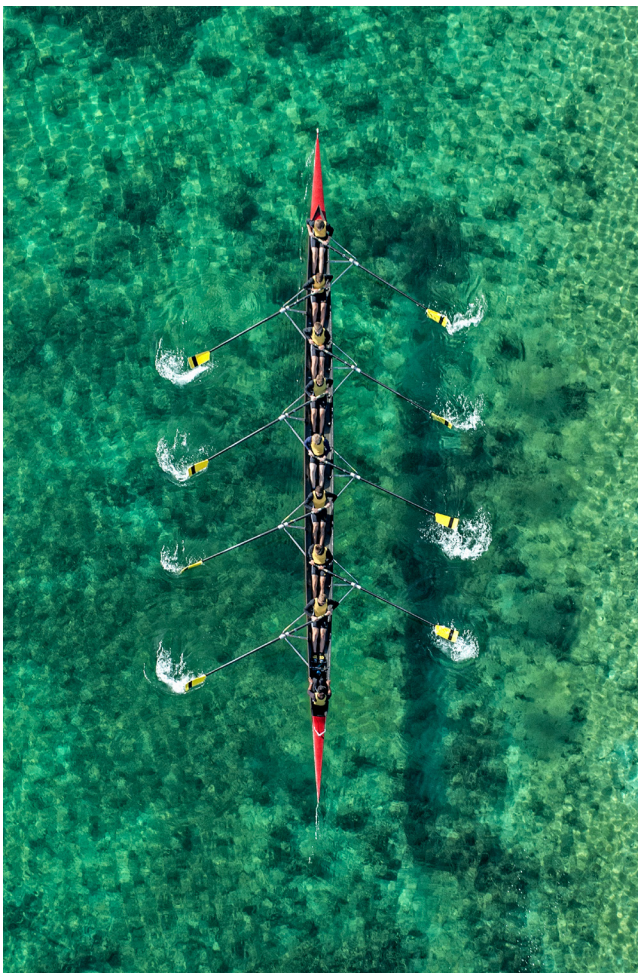
As you drill down into the specific risks and challenges facing your organization, and formulate a strategy to combat them, the framework to follow for mitigating risks and building resilience should include:

A strategic analysis of your entire supply chain: Use illumination to better understand all the critical systems and/or technology in your enterprise or products, including the parts, components, and software in your supply chain, your vendors and suppliers, all their vendors and suppliers, and the risks each could pose for your organization. Assess everything that enables your organization to operate and carry out its mission. A strategic analysis should include evaluating your supply chain provenance to understand the source of goods and materials, their chain of custody, and any potential existing concerns (e.g., cyber vulnerabilities).

A shift toward a more risk-aware and resilience-based mindset: Improve education, starting with a fully informed C-suite. Leadership should then communicate more transparently, proactively, and comprehensively, spreading cyber awareness throughout the entire organization. Be proactive rather than reactive. Even organizations that are already proactive must still do more to combat the vast array of cyber risks that can affect supply chains. Break down silos to ensure that relevant data is shared within the organization, and leveraged strategically, to help improve intelligence and resilience. Risk concerns and requirements should be built into every procurement for your vendors to respond to.

Thorough and pervasive scenario planning: Identify all the possible risks, and deploy scenario planning to assess how these risks may affect you. Use these scenarios to proactively plan ways to minimize the damage, while simultaneously preparing for the worst. Next, conduct rigorous forward planning to address any potential threats or vulnerabilities before they're able to have an impact. This could include mitigating the impacts of changing circumstances via strategic sourcing, such as moving infrastructure to alternative locations, increasing the number of suppliers, and looking into adjacent markets for vendors. Strategies like these will be necessary for organizations facing new regulations against dealing with certain companies and areas of China, for instance. Organizations unable to source the same parts elsewhere may have to retroactively adjust their supply chain to continue production, which adds additional challenges.

Robust systems and processes: Zero-trust architecture and continuous monitoring can identify anomalous behaviors and limit impacts. Put backup, disaster recovery, and contingency plans, and other risk mitigation measures in place. These steps can significantly decrease the impact of cyber threats on your organization.



INTEGRATE CYBERSECURITY INTO A LARGER SUPPLY CHAIN RISK MANAGEMENT PROGRAM

Supply chain disruption can have a devastating impact on day-to-day operations, business continuity, customer relationships, your public reputation, and more. It is essential to take consistent action to secure all facets of your supply chain, and to regularly re-evaluate threats to prevent significant adverse effects on your organization. Cyber risk is just one of many issues that can disrupt an organization's supply chain, but improving your cybersecurity posture can help to reduce risk in almost every other area, too. Cybersecurity, including the adoption of a zero-trust architecture and continuous monitoring, should be part of an overall supply chain strategy that includes illumination, assessing supply chain provenance, scenario planning, devising backup plans, and strategic sourcing.

Guidehouse experts have backgrounds in cybersecurity, supply chain security, corporate espionage prevention, information protection, intelligence, law enforcement, information analysis, and investigations. Guidehouse has the cybersecurity and supply chain risk management expertise, capability, tools, data, and best practices necessary to provide both government and industry with deeper insights into their supply chain.

ABOUT GUIDEHOUSE

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit www.guidehouse.com.

OUR EXPERTS

Jason Dury
Director, Cybersecurity
jdury@guidehouse.com

© 2023 Guidehouse Inc. All rights reserved. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. GH-224 WP Supply Chain Resilience Amid Cyber Concerns