The Growing Cyber Risk to Supply Chains

Many corporate leaders regard cybersecurity as an internal IT problem that can be delegated and forgotten. But as AI and automation reshape global supply chains, cyber readiness has become an operational capability, similar to quality or safety, with the goal being continuity in the face of disruption.

By Marko Kovacevic and Sasha Pailet Koff

NEW YORK – As the current war in the Middle East intensifies, governments and security experts have warned that the conflict could spill into cyberspace. Businesses and supply chains, particularly those in the United States and allied economies, may face retaliatory or asymmetric cyberattacks from Iran or affiliated groups seeking to exert pressure beyond the battlefield. Against this backdrop, the cyber resilience of global supply networks is no longer a theoretical concern but an urgent operational priority.

For decades, supply chains were engineered primarily to minimize cost and maximize speed and scale. Cybersecurity was often treated as an afterthought – a technical safeguard with no bearing on operational decisions. But in today's AI-enabled, data-driven economy, that is no longer true. Cyber readiness and supply-chain operations are now deeply interconnected.

Supply chains have become adaptive digital ecosystems, rather than linear flows of goods. Networks of manufacturers, logistics providers, software platforms, and data services are built on shared systems, APIs, and cloud infrastructure. AI-powered autonomous decision engines have accelerated integration by automating planning, procurement, forecasting, and execution.

While this architecture delivers extraordinary efficiency, it also creates systemic fragility. Supply-chain disruptions are increasingly triggered not by weather events or labor disputes, but by cyber incidents that compromise data integrity, system availability, and mutual trust. These incidents often originate outside the enterprise – at suppliers, service providers, or software vendors whose capabilities and resources vary widely. Attackers often target smaller, under-resourced firms as entry points into larger organizations.

In November, Marks & Spencer reported approximately $300 million in losses after a ransomware attack (initiated through a vendor) forced it to suspend online operations and left store shelves understocked. Recent attacks affecting organizations such as Jaguar Land Rover, Victoria's Secret, Toyota, British Airways, Applied Materials, Ticketmaster, and Asahi continue to show how vulnerable global business ecosystems remain. According to the 2025 Verizon Data Breach Investigations Report, 30% of breaches now involve a third party, a 100% increase from the 15% reported previously.

The result is a form of operational risk that is no longer confined to the edges of supply chains and cannot be managed by traditional governance models. For corporate leaders, cybersecurity has become an intractable challenge that technology alone cannot solve. Instead of an internal IT problem that can be delegated and forgotten, it must be addressed as a core business discipline, reinforced through culture and behavior.

The paradox of the modern supply chain is that it is powered by automation, but governed by human discretion. Every day, thousands of individuals – from procurement officers at corporate headquarters to warehouse managers at an upstream supplier – make decisions that render systems more resilient or vulnerable.

AI exacerbates this dynamic. Automated systems depend on uninterrupted flows of trustworthy data. When data are compromised or manipulated, disruption can cascade rapidly, negatively influencing planning and execution processes and amplifying errors at scale. Generative AI has also increased the effectiveness of social engineering. Instead of hacking code, attackers can now "hack" employees, exploiting trust by convincingly impersonating vendors, executives, or colleagues.

Thus, no organization can ensure cyber readiness on its own. Managing these threats requires collaboration with stakeholders of varying capabilities and maturity levels across the supply-chain network. Corporate leaders should treat cyber readiness as an operational capability, similar to quality or safety, with continuity under stress as the goal. Are their firms prepared to avert, withstand, and recover from cyber disruption across their supply chains? Can they keep goods moving, data reliable, and partners aligned even when systems are compromised?

A defining characteristic of a cyber-ready supply chain is executive accountability. Leaders must take ownership of this issue, integrating cyber scenarios into enterprise risk management and establishing clear responsibilities during incidents.

Moreover, expectations across the ecosystem must be standardized and practical. Rather than imposing complex, compliance-heavy requirements, leading organizations should define baseline practices – such as access controls, patching discipline, employee-awareness training, and incident reporting – that suppliers can realistically meet. They should also provide resource-constrained partners, including those supplying essential raw materials, with human-centric training and peer-to-peer mentorship.

Just as consistency matters more than perfection in a cyber-ready supply chain, readiness matters more than prevention. Cyber incidents are inevitable. Organizations must invest in redundancy, segmentation, backup systems, and tested recovery plans to ensure that a disruption in one link does not bring down the entire operation. They should rehearse these incidents as they would natural disasters or logistics failures.

Clear communication and support for smaller partners help cultivate trust – another essential element of a cyber-ready supply chain. When incidents occur, organizations should emphasize speed and transparency over blame, because concealment only magnifies damage in interconnected systems.

Finally, cyber readiness must be embedded in workflows. Vulnerabilities arise when employees are forced to circumvent security controls to meet operational targets. Managers must ensure that efficiency pressures do not create incentives for shortcuts.

There are immediate steps that corporate leaders can take to start building a cyber-ready supply chain. They can map critical dependencies, focusing on where digital integration and data exchange are most essential. That means identifying which partners, systems, and data flows would cause the greatest disruption if compromised – and the most important human touchpoints, where decisions are made, data change hands, and pressure to move fast is highest. With this information, business leaders can devise baseline expectations and create supports for their most resource-constrained suppliers.

As AI, automation, and geopolitical complexity reshape global supply networks, cyber risks will continue to evolve and grow. Preparing for them is no longer optional. Firms that develop cyber readiness will be more likely to retain supply-chain continuity and competitive advantage; those that do not risk becoming operationally brittle in an increasingly volatile world.

This article previously appeared on the commentary website Project Syndicate

Marko Kovacevic is Managing Director of Digital Supply Chain Institute, a nonprofit research institute focused on the evolution of enterprise supply chains in the digital economy. Sasha Pailet Koff is Managing Director of the Cyber Readiness Institute, a nonprofit organization that improves the cyber readiness of small- and medium-size businesses.