Supply chains under (cyber) attack

Cyberattacks are crippling supply chains and exposing hidden vulnerabilities in the very technologies meant to drive efficiency. As cloud platforms, robotics, and connected systems expand, companies must treat cybersecurity as a core supply chain function, building redundancy, resilience, and cross-functional defenses to withstand the next inevitable strike.

By Dr. Miguel Rodríguez García & Dr. Eva Ponce

Dr. Miguel Rodríguez García is a research scientist at MIT CTL, where he leads the Warehouse of the Future Initiative. He can be reached at miguelro@mit.edu.

•

Dr. Eva Ponce is a research scientist at MIT CTL, and she is the Director of the Omnichannel Supply Chain Lab. She can be reached at eponce@mit.edu.

In June 2025, one of the largest grocery distributors in North America, United Natural Foods Inc. (UNFI), suffered a paralyzing cyberattack. As the company's fulfillment systems were brought to a halt for almost 10 days, multiple stores across the U.S. reported shortages. This meant empty shelves at many Whole Foods locations, one of UNFI's major customers.

The financial loss because of the disruption was estimated to be at least $350 million in sales for UNFI, plus extra costs incurred as the company transitioned to manual operations and the millions spent on external cybersecurity and legal experts to solve the issue[1].

Earlier this year, Google's Threat Intelligence Group warned of a cybercrime wave that had crippled multiple British retailers and was then targeting U.S. firms' supply chains. The timing was no coincidence. Sophisticated attackers, whether organized crime or state-sponsored groups, have turned their sights to modern supply chains.

A perfect storm of vulnerability

Modern supply chains have never been more exposed. In our most recent

research, we identify at least 48 technology-related vulnerabilities in modern supply chains, and this is limited to warehouse technologies only[2]. In the broader supply chain, the number would be much higher. The tools that have made supply chains faster and more efficient, such as cloud software, IoT devices, and AI-powered automation, have also opened new doors for malicious actors.

The incidents above follow a growing list of cyber disruptions that have hit supply chains recently. In late 2023, an attack on Ace Hardware shut down its warehouse management system (WMS), halting fulfillment nationwide and causing multi-million dollar losses. As companies connect their main software such as ERP or WMS to a growing web of third-party platforms and robotics systems, the number of entry points for potential cyberattacks increases exponentially. Every new integration, API, and remote access point is a new vulnerability for modern supply chains.

In late 2024, Blue Yonder's cloud platform, used by Morrisons and other major retailers, was compromised by a cyberattack. This forced a return to manual processes in most Morrisons' UK warehouses. Simultaneously, Starbucks stores in the U.S. were also impacted by the same attack, showing how a single cyber event can bring global operations to a standstill. An attack in a cloud environment no longer remains confined to one server and can easily freeze a conveyor belt, stall an autonomous forklift, and corrupt inventory data across multiple locations all at once.

Weakest link, widest impact

The 2024 Blue Yonder attack exemplifies the domino effect of cyber risk. The global nature of modern supply chains means that attacks propagate faster than ever. When one node is hit, the ripple effects will not only disrupt upstream suppliers and downstream clients, but also third-party logistics providers (3PLs) and competitors that share technology suppliers[3].

The rise of both Software-as-a-Service (SaaS) and Robotics-as-a-Service (RaaS) has democratized access to technology. In supply chain operations such as trucking and warehousing, small and mid-size firms without previous cybersecurity knowledge are now incorporating many technologies they could not afford five years ago. These newer entrants can become soft targets, and once breached, serve as gateways to larger networks. Unless firms couple the uptake of new technology with increased cybersecurity, this democratization of technology presents serious cybersecurity risks that could outweigh the benefits of the technology itself.

However, it's not just small users of supply chain technology that increase cyber exposure, it's also the rapid proliferation of small tech companies introducing new software, robots, and platforms into critical operations. Companies in early stages will often prioritize speed to market and innovation over robust security architecture. While they bring agility and functionality, their solutions may lack hardened protocols, comprehensive

security testing, or dedicated cyber teams, inadvertently injecting risk into new supply chain technologies.

What can companies do?

Resilience begins with recognition: cybersecurity is now a supply chain issue, not just an IT concern. Based on more than 40 interviews with experts across industries, we have identified several best practices:

Scrutinize your supply chain tech portfolio. As supply chains increasingly depend on third-party providers for cloud platforms, robotics, analytics dashboards, and IoT infrastructure, companies must establish clear cybersecurity requirements for all partners, audit them regularly, and restrict system access to the minimum. For example, over-the-air (OTA) updates, which are a growing norm not only for our mobile phones but also in robotics, can be exploited if not verified properly. Moreover, firms should demand transparency from vendors on their response protocols, for both software and physical automation and robotics, when operating under SaaS or RaaS agreements.

Don't bet the supply chain (and business) on one system. Single points of failure can be catastrophic. We now know that the WMS can be a critical software not just for a single warehouse, but for entire supply chains. When the central brain that connects all nodes goes down, everything stops. The cases of Ace Hardware and Morrisons are a reminder that companies must build redundancy. That could mean keeping multiple copies of critical systems running in parallel. For instance, even if the main system is cloud-based, companies could use a backup copy working on-prem or an edge cloud approach, with additional layers of protection and an isolated network that can function in offline mode.

Speed kills (when companies skip security). Many companies rush the implementation of new facilities across supply chains to hit commercial deadlines. Something similar happens during mergers and acquisitions (M&A) when supply chains integrate. Our research has shown us that when this happens, cyberattacks are both more frequent and more successful, as cybersecurity often becomes an afterthought. This is especially true in peak seasons when IT resources are stretched thin and the company's priorities are focused on daily operations. Cybersecurity must be part of every technology rollout checklist from day one, not a patch added later.

Resilience must be built. Modern business continuity plans (BCPs) must assume that cyberattacks will happen, and that they may take days to resolve. Redundancy, shutdown protocols, backup systems, offline access,

and detailed restart playbooks are critical. Leading companies interviewed for this article emphasized the need to test BCPs regularly, not just on paper but in practice, simulating real-world cyber scenarios not only among IT folks, but hands-on with their operations teams. Having dual WMS servers or local data caches can make the difference between a temporary slowdown and a total standstill. Partnerships with institutions like MIT CTL can help companies push this further by developing simulation environments that translate cyberattacks into physical disruptions across supply chains, enabling decision-makers to rehearse outages, identify gaps in recovery protocols, and build response strategies.

A final word

Cyber risk is now a structural threat to supply chains. The more connected we become, the more we must invest in securing those connections. And still, companies need to prepare for operating in the dark and build resilience in their IT and physical supply chain systems, as prevention strategies alone will not be enough.

But companies shouldn't do this alone. It's time for supply chain and cybersecurity leaders to collaborate more deeply—not just reactively after a breach, but proactively as part of the supply chain design process itself. Moreover, institutions like MIT CTL can convene firms' interests and create a secure space that brings together government agencies, key stakeholders, and industry leaders, aligning industry priorities with MIT's research agenda. •

•••

References

1. Silverstein, S. (July 16, 2025). "UNFI expects cyberattack to cost it at least $350 million in sales." Cybersecurity Dive. Available at https://www.cybersecuritydive.com/news/unfi-cyberattack-losses-insurance-grocery-distribution/753224/. Accessed September 25, 2025.

2. Rodríguez-García, M., Kembro, J. H., Betts, K., & Ponce-Cueto, E. (2025). "Managing technology-related disruptions and vulnerabilities in highly automated warehouse systems: an integrative review and research agenda." International Journal of Production Research, 1-33. https://doi.org/10.1080/00207543.2025.2552281.

3. Brown, M. (September 3, 2025). "Why supply chain cybersecurity still falls short and what leaders must do next." Supply Chain Management Review. Available at https://www.scmr.com/article/why-supply-chain-cybersecurity-still-falls-short-and-what-leaders-must-do-next. Accessed September 25, 2025.