Why are we getting supply chain cybersecurity wrong?

Miguel Rodríguez García is co-founder and director of the Supply Chain Cybersecurity Lab at the MIT Center for Transportation & Logistics. He can be reached at miguelro@mit.edu.

Treating cybersecurity as an IT responsibility leaves physical operations exposed. MIT research points to the need for shared expertise, operational response plans, and earlier communication across supply chain partners.

By Miguel Rodríguez García

Research has consistently shown that supply chain risk management is often late to new risks[1]. It is part of human nature: we learn from experience and calibrate our risk tolerance based on what we know and what we have already faced. When a disaster occurs, companies respond, and they prepare for the next version of the same event.

But what happens when the risk is something most supply chain teams have never confronted at scale?

That is exactly where we stand today with supply chain cybersecurity. AI-enabled cyberattacks are multiplying the speed and frequency of these disruptions. At the same time, supply chains depend more than ever on interconnected

software, cloud platforms, robotics, artificial intelligence (AI), and complex networks of technology providers, even as many still rely on legacy systems with low levels of cybersecurity protection.

Our ongoing global study on supply chain cybersecurity at MIT is showing how firms are struggling to fight these emerging risks, and the reasons are technical, behavioral, organizational, and managerial.

Several challenges stand out.

'That's an IT problem, not a supply chain problem'

Among supply chain professionals, there's a significant lack of both attention to and knowledge about cybersecurity.

For decades, supply chain professionals have neglected cybersecurity because it hasn't been part of their daily work. For most professionals, cyber risks are the domain of IT or cybersecurity teams alone. The result is a systematic failure to build the cross-functional knowledge needed to manage supply chain cybersecurity risks at scale.

Research has shown that a company's behavior is shaped by how organizations channel and distribute the attention of their decision-makers. Sustained attention is known to be the prerequisite for expertise: only what gets focused on gets acted on[2].

This means that when supply chain professionals do not regularly engage with cybersecurity, they do not develop the situational awareness to recognize early warning signs or make sound decisions under pressure.

In our ongoing research, we have found that:

1) Supply chain professionals view cybersecurity as too complex a problem, since most lack a background in information technology (IT).
2) Organizations do not encourage managers to allocate enough time to this cross-learning. Procedures, performance reviews, meeting agendas, and incentives for most supply chain professionals do not create space for their teams to think about cybersecurity.
3) The lack of cross-functional knowledge is critical because cybersecurity teams hold the knowledge of the digital layer, but operations teams understand how the physical flow of goods depends on those digital systems.

For instance, one of the companies we studied recently lost its transportation management system (TMS) provider due to a severe cyberattack. During the disruption, the only reason the firm could keep managing its transportation carriers was that a significant portion of the team knew how to do the same work in Excel, as it had been done several years before the attack. The company was lucky the team held this knowledge.

Most incident response playbooks, owned by IT or cybersecurity teams, do not manage granular operational steps, but instead serve as high-level decision frameworks that trigger a business continuity plan (BCP). The tactical, operational tasks like rerouting trucks or switching certain operations back to manual are still the duty of supply chain teams, although our research shows they are rarely part of the BCPs.

Nobody talks

Another challenge is how reluctant firms are to talk about supply chain cybersecurity, both internally and externally. Both supply chain and cybersecurity professionals avoid disclosing and discussing incidents, even in conversations with trusted third parties like MIT that can offer anonymity. Reputational risk and legal exposure pose strong structural barriers to sharing information about disruptions[3].

No company wants to admit what they have done wrong. Sometimes legal teams prohibit disclosure, while in other cases people are simply reluctant to discuss mistakes. Research has shown that few organizations develop a culture of self-reporting mistakes to encourage disclosing and learning from failures. This presents a significant barrier to cross-organizational learning in cybersecurity.

More surprising, we found the same lack of transparency within companies' own supply chains. For instance, several technology suppliers noted that they are often afraid of being punished if they report a cyberattack to their clients, so they tend to delay disclosure until they have confirmation that the issue is in fact a cyberattack. This can cause tremendous damage to the overall supply chain, as warning time is critical: the sooner a disruption is communicated, the more time partners have to isolate and shut down systems correctly, actively fight the threat, and activate alternatives.

So why don't client firms prescribe more specific security practices or protocols to their suppliers, for instance, regarding communication? It turns out that clients are afraid of being held legally responsible if they provide guidance and one of their suppliers gets hacked, as this could shift accountability for third-party liabilities onto them. As a result of this tension, nobody talks and nobody wins.

What companies can start doing about it

Whether companies face gaps in cybersecurity knowledge, barriers to discussion, or both, our research offers a few directives for supply chain professionals.

1. Envision the problem at scale.

To connect the supply chain and cybersecurity worlds, understanding how cyberattacks are already impacting global supply chains is a first, necessary step.

The new Supply Chain Cybersecurity Lab at MIT CTL is already working to solve this challenge. TRACE is a new, global database of reported cyberattacks that disrupt physical supply chain operations. Still in an early stage, the tool aims to collect large amounts of data that can bring insights into what factors are exposing supply chains the most, ultimately helping technical and executive teams understand the real operational risk of cyberattacks. TRACE can be accessed at ctltrace.com.

2. Bring supply chain professionals into the cyber world, and vice versa.

Train your supply chain teams in cybersecurity—technical training is not necessary, but at least from a tactical and systems perspective. Any supply chain professional should be able to answer what dependencies their material flows have on technology and what they would do in the case of a cyberattack.

To do this, cybersecurity teams should build BCPs together with supply chain professionals. These plans need to go beyond the IT layer and include tabletop exercises at the tactical level, which should incorporate people from the field in the discussions. These exercises can help teams work through how to mitigate and recover from a cyberattack that is impacting physical operations.

3. Create safe spaces to spark conversations and share data.

Cross-industry initiatives, such as academic research co-developed with multiple industry partners and gatherings held under the Chatham House Rule, can create these spaces. At these gatherings, like roundtables, companies can share openly without specific remarks being attributed to them.

Regarding data, we can draw inspiration from the aviation industry. NASA designed the Aviation Safety Reporting System (ASRS) in 1976 for the FAA, which is a non-punitive channel for pilots, crew, and other staff to confidentially report near misses in the interest of improving aviation safety. Researchers have proposed a similar reporting system in cybersecurity as a potential major win for the industry (including the cyber insurers), but it has never materialized. With the increase in cyberattacks we are experiencing, such a system is worth a second look.

One action won't be enough

Overall, not all the companies we interviewed suffered from all the challenges above and some of them are already moving in the directions mentioned. However, in the coming years, the supply chain cybersecurity challenge will only intensify, and one single step forward won't be enough.

After a cyberattack, the difference between halting operations for a couple of days instead of a couple of weeks could mean the survival of the business.

It's time for supply chain and cybersecurity leaders to collaborate more deeply. The new Supply Chain Cybersecurity Lab at MIT CTL welcomes the opportunity to work with industry to protect physical supply chains from cyberattacks. What other actions is your company taking to enhance its supply chain cybersecurity capabilities? We know change management is slow, so how can we accelerate it to match the rapid evolution of AI-enabled cyberattacks and the increasing technology dependency in supply chains? •

***

1. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. International Journal of Logistics Management, *15(2), 1–14. https://doi.org/10.1108/09574090410700275*

*2. Ocasio, W. (1997). Towards an attention-based view of the firm. S*trategic Management Journal, *18(S1), 187–206. https://doi.org/10.1002/(SICI)1097-0266(199707)18:1+<187::AID-SMJ936>3.0.CO;2-K*

3. Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. *Research in Organizational Behavior, 21, 81–123*