DOW JONES RISK JOURNAL

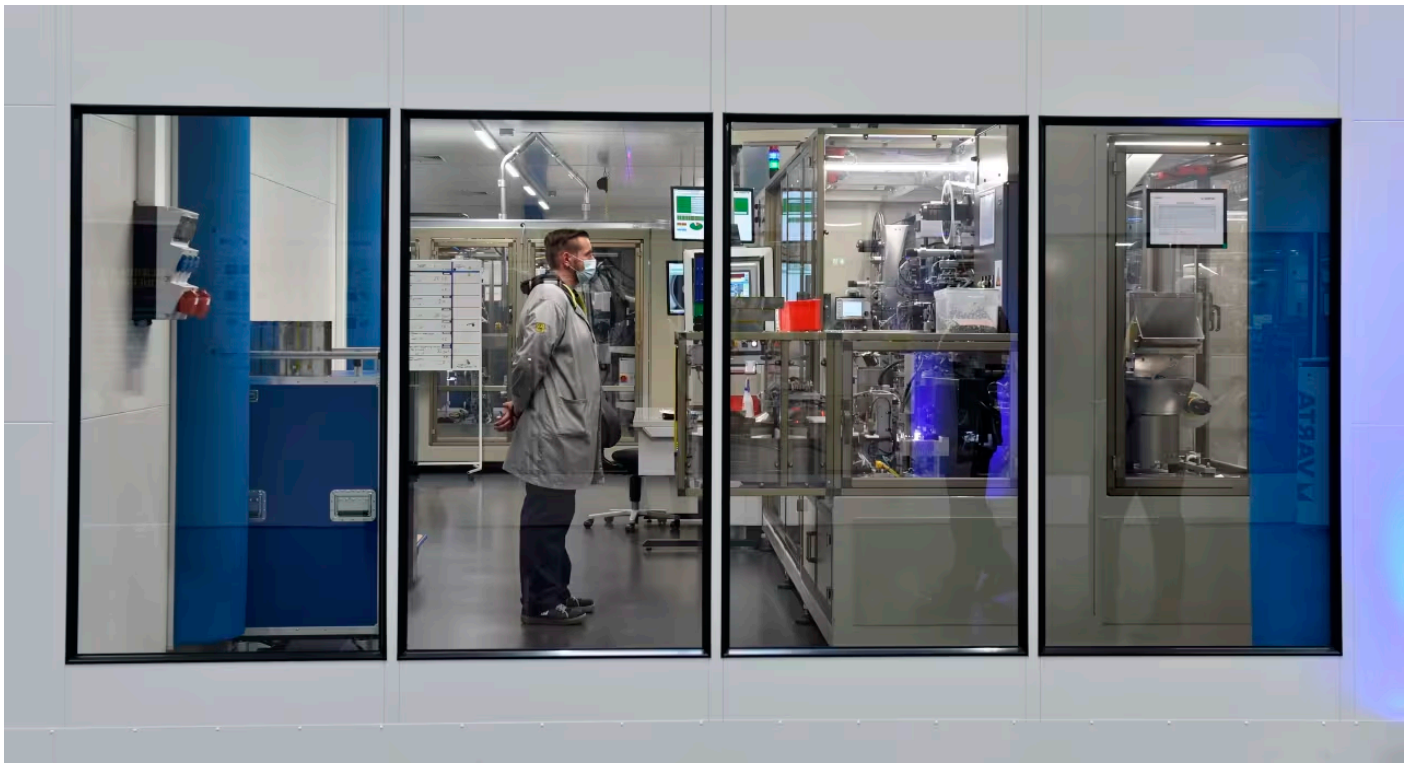
Supply Chain | Artificial Intelligence | Best Practice

The Weakest Link: Why Supply Chain Cybersecurity Starts with Small Businesses

In an interconnected supply chain, the security of every company depends on the cyber readiness of its partners

By Craig Moss

Dow Jones Risk Journal, March 30, 2026 at 04:00 AM EDT



Many manufacturers have experienced cyberattacks that forced a shutdown of IT and OT systems and halted production across plants across Europe and Asia. Photo: a production employee overseeing operational technology. PHOTO: AFP VIA GETTY IMAGES

Cybersecurity in the Supply Chain

Modern supply chains are complex networks of companies, each playing a role in producing and delivering products or services. Data is the glue that holds these networks together,

flowing continuously between companies, systems, and software platforms. Every organization involved shares a responsibility for protecting that data. Trust is essential.

While digital connectivity has made supply chains faster and more efficient, it has also created attractive targets for cybercriminals and hackers. Within a company, effective cybersecurity requires the coordination of people, processes, and technology, an arduous task. Across a supply chain, the challenge becomes even greater because the security of the entire network is only as strong as its weakest link.

Hackers understand this. Increasingly, they target smaller companies within global supply chains to use them as gateways to larger companies because the assumption is that smaller companies have fewer resources and less cybersecurity expertise. Too often, that assumption proves correct.

Horror Stories

Unfortunately, examples of supply chain cyberattacks are easy to find. These incidents demonstrate that attacks can target manufacturers, software developers, and even critical infrastructure like water utilities. They also target information technology (IT) systems and operational technology (OT) systems.

- **A ransomware attack on supplier Kojima Industries forced Toyota to suspend production in all 14 of its Japanese plants, resulting in the lost output of 13,000 cars and exposing the vulnerabilities of just-in-time supply chains.**
- **HanesBrands suffered a ransomware attack that disrupted its global supply chain, resulting in a 3-week suspension of order fulfillment. The incident caused approximately $100 million in lost sales and $15 million in remediation costs.**
- **German battery manufacturer VARTA AG experienced a cyberattack that forced a shutdown of IT and OT systems and halted production across plants in Germany, Romania, and Indonesia, causing widespread shipment delays for customers relying on just-in-time delivery.**
- **CDK Global was the victim of a ransomware attack that forced it to take its Dealer Management Systems (DMS) software offline, crippling the operations of over 15,000 North American car dealerships and disrupting vehicle sales, financing, and repairs.**
- **U.S. water utilities have been targeted as well. In Texas, hackers tampered with water pumps and alarms at two Texas water facilities. In Massachusetts, hackers gained control of chemical treatment systems for drinking water.**

These incidents illustrate a clear trend: the cyber threat to supply chains is growing, not diminishing. The challenge is enormous because supply chains consist of thousands of small and medium-size businesses (SMBs), many lacking the internal expertise or technology resources available to larger companies. Hackers know this, and they know that these smaller companies are connected to the systems of their larger customers.

Impact of AI and Agentic AI

The use of Generative AI (GenAI) and AI Agents across supply chains is introducing new opportunities, and new risks.

Unlike traditional AI or GenAI tools that respond to specific prompts, AI Agents can plan tasks, interact with other software systems, and complete projects with minimal human oversight. While these capabilities can dramatically improve efficiency, AI Agents can also provide hackers with automated ways to increase the sophistication and scale of their attacks. My previous article, *Using AI to Manage Supplier Risk,* looked at how GenAI can help scale supply chain risk management.

Because AI Agents can access systems, move data, and make decisions, they can also expose sensitive information, act on incomplete instructions, or be manipulated by malicious actors if not properly configured and monitored. The same autonomy that makes them powerful can also amplify risk. This is true with IT and OT systems.

At the same time, hackers are using their own AI Agents to automate and scale their attacks. Here are two common methods:

- **Automated Reconnaissance and Hyper-personalized Execution: Trying to attack a supply chain with 10,000 suppliers was previously a "human capital" problem—a hacker simply couldn't manually research and phish that many targets effectively. GenAI and AI Agents change the math by providing automated reconnaissance and hyper-personalized execution at scale.**
- **Prompt Injection: One of the most common risks. An attacker crafts a malicious instruction (a "malicious prompt") that tricks the AI Agent into ignoring its safety rules, revealing secret passwords, corrupting data, or performing unauthorized tasks like sending money.**

There are foundational steps that every company should take to prevent cyberattacks and reduce the impact if and when an attack occurs. Effective governance is the key.

Supply Chain Complexities

Managing cybersecurity across the supply chain shares many similarities with managing compliance and sustainability risks, from labor rights to corruption. A risk-based approach is essential because you cannot protect everything equally well. Not every supplier presents the same level of risk. The level of exposure is based on what data is shared, what systems are connected, and the criticality of what they do from a business and operations perspective.

Reducing Residual Risk

My previous article, *Leveraging Residual Risk Data to Go Beyond Reporting*, talked about the need to focus on residual risk. It is difficult or impossible to change the level of inherent risk because it is based on what an organization does, where they do it, and how they do it. What can be changed is the level of residual risk by improving the management systems and controls.

In the case of cybersecurity, reducing residual risk clearly requires a focus on people, processes, and technology. Technology alone won't sufficiently reduce risk to an acceptable level, especially across complex supply chains. Reducing cyber risk must involve human behavior.

Given the potentially severe financial and operational impacts of cyber incidents, cybersecurity has become a priority for executive management and Boards. Most large companies have invested significant resources in cybersecurity with a focus on protecting their internal systems and data. The maturity of their management systems often far exceeds those for other compliance and sustainability topics. In addition to technical controls, awareness training is often far more systemic and advanced. In many cases, compliance and sustainability departments are advised to look at the cybersecurity management systems and see where they can piggyback or replicate them. However, the cybersecurity department faces the same challenge as compliance and sustainability in managing third parties, which can number in the tens of thousands.

The Cyber Readiness Institute (CRI), a nonprofit, was founded to help address this challenge by reducing cyber risks across supply chains. Over the past eight years, with support from companies such as Microsoft, Mastercard, Apple, General Motors, and T-Mobile, CRI has developed a program dedicated to reducing cybersecurity risks in SMBs by focusing on human behavior.

Many SMBs lack the time or resources to become cyber experts or purchase expensive technology. They often outsource their IT or OT management to managed service providers

or vendors. Hackers know this and are systematically targeting SMBs as gateways to higher value targets, now using GenAI and AI Agents to scale their attacks.

“Cyber readiness begins with people,” said Sasha Pailet Koff, managing director of the Cyber Readiness Institute. “Small and midsize businesses sit at the heart of global supply chains, and their everyday security habits, using strong authentication, keeping systems updated, and verifying requests, create the first line of defense. When those practical behaviors become routine, the resilience of entire industries improves.”

To support SMBs, CRI developed the Cyber Readiness Program to demystify cybersecurity and help organizations of all sizes take practical steps to reduce their residual risk. The key elements include:

- **Appoint a Cyber Leader: every company should designate a person responsible for promoting cybersecurity awareness and building a culture of cyber readiness. This role differs from an IT person. Many SMBs outsource their IT or OT management, but they can’t outsource building the culture.**
- **Focus on the Core Four to prevent attacks:**
  - **Passwords + Multi-factor Authentication (MFA)**
  - **Software Updates**
  - **Phishing Awareness**
  - **Secure Storage and Sharing**
- **Develop an Incident Response Plan to minimize damage if, and when, an attack occurs that includes:**
  - **Prioritization of data and systems**
  - **Backup plan**
  - **Contact information and responsibilities**
- **Train the entire workforce on the Core Four and the Incident Response Plan**

CRI’s free online Cyber Readiness Program has proven effective in helping SMBs establish a basic cybersecurity culture, with 73% of the companies reporting it had a ‘high’ or ‘very high’ impact on their cyber readiness. For many companies, it serves as a useful steppingstone toward meeting more rigorous technical standards such as SOC 2 or CMMC 1, or those required by customers.

The human-centered approach is one of the reasons Christopher Cruz, Cyber Program Manager for the Virginia State Police, values the Cyber Readiness Program. It helps organizations build stronger defenses and healthier security cultures. “The targeting of humans is still such a huge part of why attacks succeed,” he says. “Doing cybersecurity well is just as much about culture as it is technology. You can have every firewall and intrusion detection system in place, but if people don’t follow procedures, you’ll always have gaps.”

Over the past two years, CRI’s program has been deployed with small and medium-size water utilities in the US. As critical infrastructure, water utilities are a high-value target for hackers. The interaction between IT, OT, and alarm systems creates several vulnerabilities that can be exploited.

Programs like the Cyber Readiness Program demonstrate that meaningful risk reduction doesn’t always require major technology investments. By focusing on human behavior and practical habits, organizations can significantly strengthen supply chain resilience.

Call to Action: Prioritize

No organization can protect everything equally well. The key is understanding what matters most. This is true internally and in the supply chain.

A simple and effective way to prioritize is to think of two inherent risk buckets:

- **Data Loss: What data would be the most damaging to lose, go public, be corrupted or not be able to access?**
- **Business Continuity: What IT or OT software or hardware would cause the most damage to operations if they went down?**

While these questions may already be answered internally, the questions must be asked of the direct suppliers and down the supply chain beyond the direct suppliers. Data loss and business continuity incidents can be caused by any company at any level in the connected supply chain. Every company in the supply chain is impacted if one company goes down.

Hackers will always look for the weakest link. Prioritization is the critical first step in knowing where to focus resources and improve program maturity and reduce the residual cybersecurity risk.

In today’s interconnected supply web, risk management cannot stop of at the boundaries of a single company. It must be extended across the supply chain using a risk-based approach, ensuring that every partner is taking the practical steps to improve cyber resilience. As AI

Agents become more prevalent in supply chain management the inherent cybersecurity and data loss risk will escalate. In response, companies must collectively take practical steps to reduce the residual risk and strengthen the weak links.

—Craig Moss is a director at the Digital Supply Chain Institute and the Cyber Readiness Institute, executive vice president of measurement at Ethisphere and a board member of the Association of Professional Social Compliance Auditors.