



5 Ways to Shield the Electronics Supply Chain From Cyberthreats

Five practical steps electronics companies can take to reduce supply chain cyber risk.

The electronics supply chain has become a prime target for cybercriminals because it moves sensitive information across many systems, depends on third-party access and is only as secure as its least-protected supplier. When one partner slips, the ripple effects can travel quickly across connected systems and teams. This is why companies should be paying close attention to the weakest links in those connected, expansive supply chains.

Supply chain attacks as a whole have been increasing since early 2025, when [Cyble's dark web researchers](#) observed claims of 31 such attacks. Since then, cyberattacks with supply chain implications have averaged 26 a month. Each incident has the potential to impact many downstream customers, Cyble warns, with one ransomware group claiming that a recent attack yielded data on 41,000 customers of a company. "Ransomware attacks, data breaches, zero-day exploits and IP theft have been among the recent incidents impacting the supply chain," it adds.

The attacks often start at the micro level, with a compromised login at a component supplier, for example. From there, it moves into shared tools like supplier portals where design files, bills of materials and pricing data are shared. Before long, that access can extend into enterprise resource planning (ERP) environments that support ordering and fulfillment. And with that, a single issue can quickly ripple across manufacturers, distributors, logistics partners and other stakeholders.

"Electronic supply chains are complex. They involve a mixture of suppliers, sites and software tools. Each link contributes to some weakness," Priya Bhalla writes in "[Cybersecurity Considerations for Electronics Supply Chain Management Systems](#)." "These systems are targeted by attackers, who can have a large impact. One breach can halt production, retard delivery, or open key product designs. Even small-scale disruptions can be costly in time and money."

Here are five things organizations can do now to close common cybersecurity gaps in electronics supply chains:

1) Know your own systems. It sounds fundamental, but strong cybersecurity really starts with knowing your systems. For best results, Bhalla says companies should maintain a clear view of the software programs they use, who can access them and where the data is stored. "Access control plays a big role," she adds. "Users should only have access to what they need to do their job. This limits damage if an account is compromised."

2) Use clear data rules. Data is the core of supply chain management and includes supplier details, pricing, product designs and production plans. "If this data is exposed or changed, the impact can be serious," says Bhalla. She recommends encryption as a simple but powerful tool. "Data should be encrypted when stored and when shared," Bhalla says. "This helps keep information safe even if it's intercepted."

3) Recognize, map and prioritize the threats. The first step in implementing supply chain security is assessing all possible risks, and that means understanding the supply chain and its key components by inventorying suppliers and assessing their security posture. [BlueVoyant](#) recommends grouping vendors into risk profiles; prioritizing each third party by their vulnerability level, access to your data and systems and impact on your organization; and using questionnaires and onsite visits to assess supply chain security. "Identify the weakest areas in the supply chain," it adds, "and supplement these vendors or ask them to improve their security."

4) Get everyone onboard with the cause. The bad actors have different motives ranging from ransom to sabotage to intellectual property theft. And their attacks can take many forms, such as malicious code injections into legitimate software, hijacking software updates or attacks on IT and operational technologies. "As cyberattacks increase, supply chain leaders need to coordinate with security and risk management leaders to understand these threats," [BlueVoyant](#) says. "All leaders should work together to jointly manage supply chain security risks."

5) Always be monitoring. Lastly, [IBM](#) tells companies to put time and effort into developing a well-defined, adaptable, data-based approach to cybersecurity. By conducting regular risk assessments, establishing and following security protocols, and continuously monitoring the situation, companies can stay out in front of the problem and avoid the biggest risks. "Regularly review and update your cyber risk management policies to ensure they are up-to-date and relevant," it adds. "This will help you stay ahead of evolving threats and maintain the security of your supply chain."