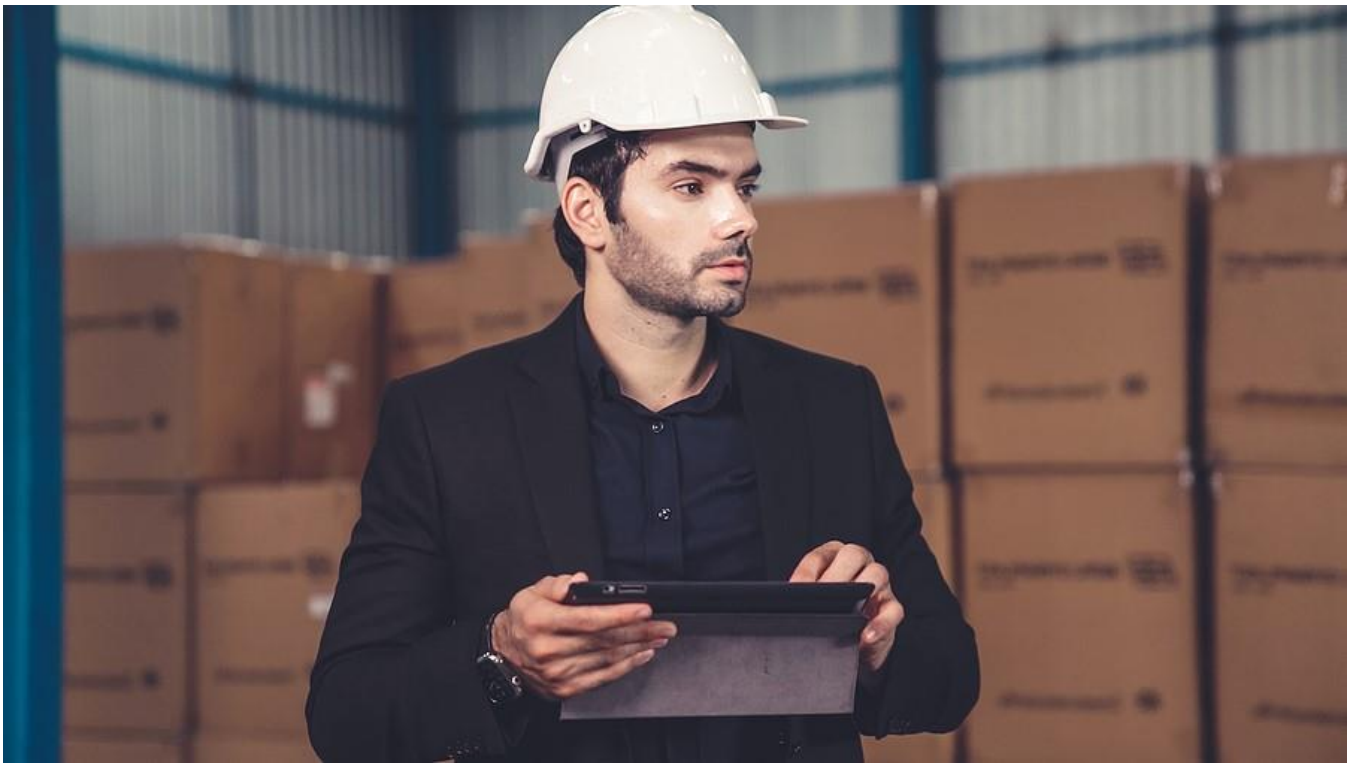
Manufacturing Cybersecurity Issues and What to Do About Them



Smart manufacturing techniques have driven productivity and innovation, improved product quality and boosted efficiency. But connected systems also bring increased risks. Manufacturing cybersecurity issues such as aging systems and supply chain vulnerabilities open the door for malicious actors.

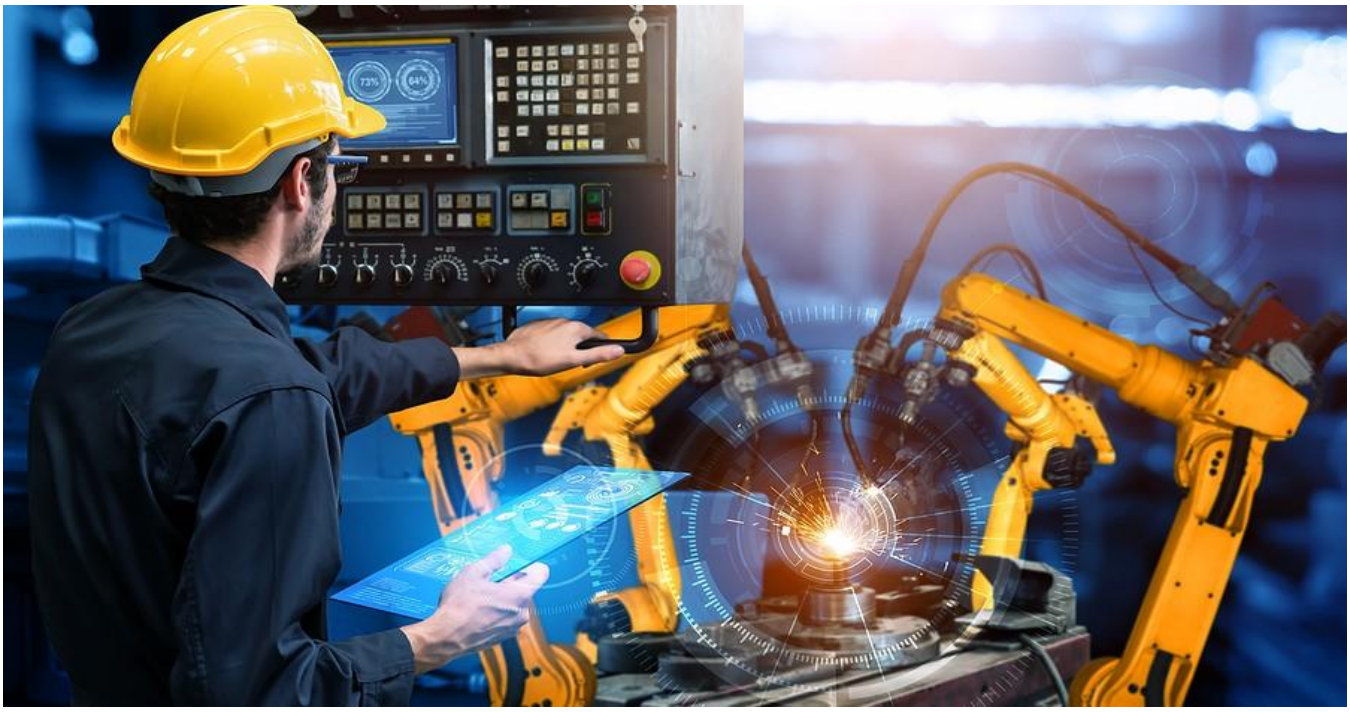
In fact, a recent report from IBM indicates that manufacturing took over as the most attacked industry in 2021. Manufacturing poses an attractive target for several reasons. For instance, difficult-to-patch systems leave vulnerabilities for attackers to exploit. Additionally, disruptions to the supply chain make manufacturers more likely to pay ransoms.

Out-of-date Systems Put Critical Work at Risk

Manufacturing processes depend on intricate, specialized machinery. Critical pieces of many systems have been in place for years, implemented before the need for internet connectivity. Consequently, it can prove difficult to keep key pieces of machinery up to date, leaving them vulnerable to exploitation.

For instance, although Microsoft stopped supporting Windows XP eight years ago, an estimated seven percent of the world's computers still run XP. With a host of known vulnerabilities, XP puts these computers and the networks they run on at risk of attack.

Still, updating old systems can be a complex process, often creating a ripple effect, so some organizations continue to delay. Unfortunately, according to IBM, unpatched software accounted for nearly half of attacks on manufacturing in 2021.



Supply Chains Create Possible Back Doors

Supply chains have been causing headaches in recent years for several reasons. In terms of cybersecurity, an interconnected supply chain gives attackers multiple points of possible entry into the corporate network.

For example, even though the main target may implement good cybersecurity controls, weaker organizations in the supply chain can prove easier to breach. And when vendors perform maintenance to manufacturing systems via remote access, the process opens additional entry points. Hackers exploit this access to install malware and conduct espionage.

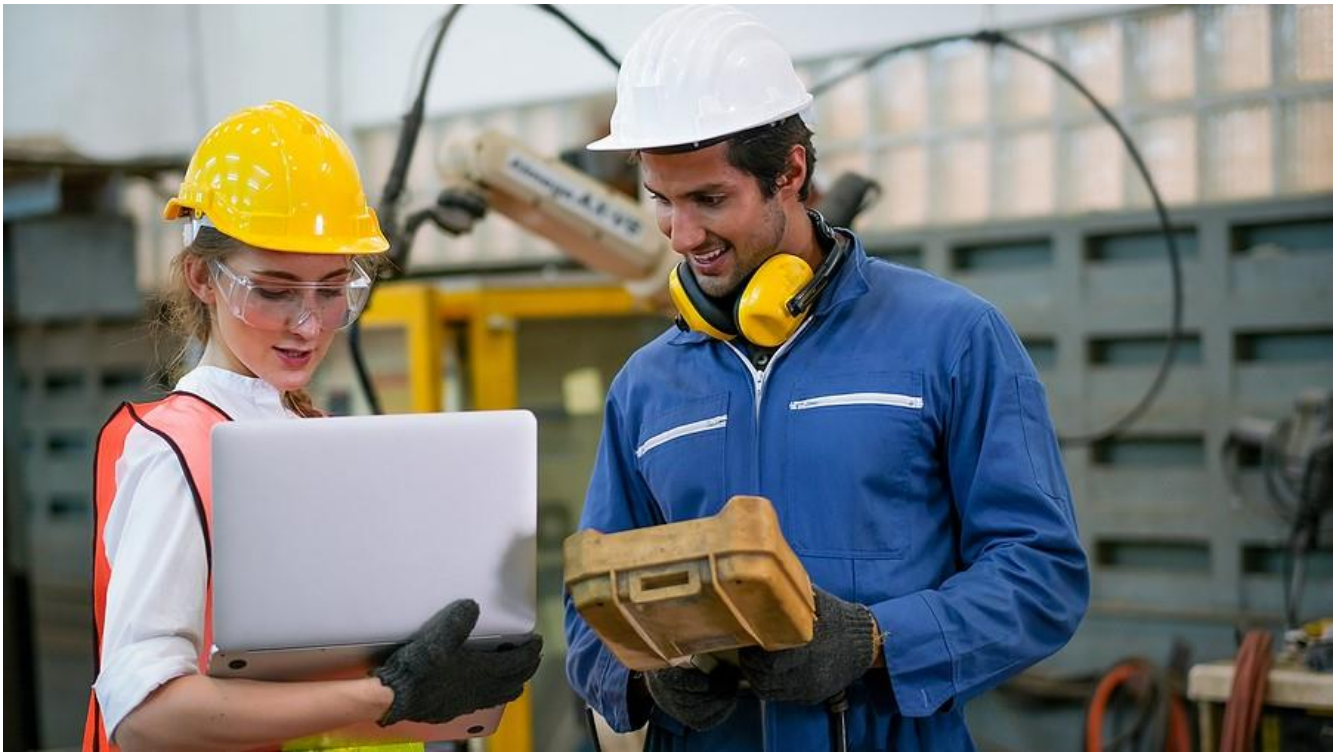
Additionally, hackers take advantage of the trust that organizations have for companies in their supply chain. With stolen credentials from a vendor, they can impersonate a trusted source and launch a successful spear-phishing campaign.

Solutions to Address Manufacturing Cybersecurity Issues

With so much at stake, manufacturing companies need to take a closer look at their cybersecurity programs. Start with a few critical cybersecurity best practices, such as the following:

- **Keep systems up to date** – Implement a patch management system, beginning. with a thorough inventory of existing systems. Wherever possible, apply security patches without delay. When a device does not allow for updates, isolate it from the main network to reduce risk of infection.

- **Segment your network** – Breaking the network into smaller segments reduces risk by limiting lateral access within the organization. It also allows the security team to implement network access controls and appropriate security measures more easily.
- **Have backups** – In addition to data backups, consider having backup machines in case a critical piece of the system goes down.
- **Better collaboration between OT and IT** – With connected systems, OT and IT can no longer operate in separate siloes. Adjust roles and responsibilities as necessary to foster a closer working relationship between OT and IT functions.



- **Deploy malware detection** – Combine antivirus and anti-malware solutions for maximum protection. A good anti-malware program will detect and patch even zero-day vulnerabilities. Keep both up to date to stay abreast of new attacks.
- **Vet your supply chain thoroughly** – Assess the cybersecurity programs in use at the companies in your supply chain. Make sure they implement proper security controls and that they meet regulatory standards.
- **Implement basic cybersecurity** – Revisit basic cybersecurity principles. For instance, implement multi-factor authentication and encryption, enforce strong password rules and provide regular security awareness training.

The manufacturing cybersecurity experts at eMazzanti provide the essential tools and expertise necessary to secure manufacturing operations. Beginning with a security assessment to identify vulnerabilities, they will tailor a cybersecurity solution to your needs and budget.