The digitalization of manufacturing is transforming the industry, from better insights to real-time information to improved efficiencies, but it has also created vulnerabilities. While providing considerable benefits, like reduced downtime and streamlined troubleshooting of machines, connected manufacturing also creates more potential points of entry for threat actors. These vulnerabilities encompass a range of entry points, including equipment, legacy systems, IoT devices and more, and the effects can significantly impact the supply chain. Smart manufacturing is the future, but manufacturers must proactively defend against cyber threats as they continue to digitize in order to reap the benefits of Industry 4.0.

The challenges of digital transformation

The manufacturing industry faces unique challenges when it comes to digital transformation. Over the years, numerous non-standardized systems have evolved independently of each other, fragmenting manufacturing systems and creating data silos. For manufacturers, digital transformation takes more effort than it does for companies in industries operating largely in digital environments. Connecting physical systems and objects — production lines, machinery, equipment, materials, etc. — to networks in often hazardous environments adds another layer of difficulty.

Interoperability, or the lack thereof, is also a challenge. Industrial settings are often characterized by disparate systems that do not interface with each other. This setup leads to silos of data, which strengthens the case for digital transformation while simultaneously making the process more difficult. As a result, implementation is often piecemeal.
Since the barriers to entry are higher for manufacturers and their risk aversion is so high (so as to avoid non-scheduled downtime and maintain production/quality targets), they can tend to lag behind other industries. And because the manufacturing industry is less advanced in its digital transformation, manufacturers are less likely to fully understand the risks and how to mitigate them. It is also worth noting that enterprise cybersecurity practices and principles have not consistently made their way through to the operational technology side in many manufacturers. Understanding the cyber threats is important for mounting a cybersecurity defense in any industry, but it’s crucial in manufacturing.

**Ransomware on the rise**

The vast majority of threat actors in manufacturing (96%) are financially motivated. It should come as no surprise, then, that ransomware, which accounts for a large portion of the breaches in the system intrusion pattern, has been on the rise in manufacturing for three years in a row. Ransomware is an increasingly lucrative action type for hackers. The median cost per ransomware more than doubled over the past two years to $26,000, with 95% of incidents that experienced a loss netting hackers between $1 million and $2.25 million.

This is particularly worrying for manufacturers. Ransomware is often used to obtain sensitive information in order to extort funds. In manufacturing, however, ransomware can be used to hold a production line hostage. Every minute a production line is down, a manufacturer hemorrhages money. Since manufacturers cannot afford to experience extended downtime, the pressure to comply with even the most exorbitant demands is high. Ransomware poses a great risk for manufacturers, a risk that is only growing.

**Denial of Service can halt an entire production line**

Denial of service attacks, in which network users are denied access to information systems, devices, or other network resources, are very common in manufacturing. DoS attacks, which have been trending upward over the last few years, account for two-thirds of incidents in this vertical. In manufacturing, DoS attacks can be used to shut down machines or entire production facilities. With cybersecurity intrusions on the rise, manufacturers can ill afford to see their operations shut down for an extended period of time. As such, this approach can pose similar threats to ransomware.

**Investing in technology solutions and in your people**

*Network detection thwarts and contains*

Network detection and response provides greater visibility of a network, threat detection and forensic analysis of suspicious activities. It markedly accelerates a manufacturer’s ability to respond to attacks and identify future attacks before they become serious events. It’s also effective for defending against lateral exposure, which
is especially critical for a manufacturer that has connected its entire ecosystem, from production to packaging to supply chain.

**Education’s role in prevention**

The impact of the human element on cybersecurity cannot be overstated, factoring in the overwhelming majority of incidents and almost three-quarters (74%) of total breaches. Social engineering, a malicious tactic in which users are tricked into divulging a network’s sensitive information, is commonly used to gain entry into a network in order to install ransomware or other malware. Making sure the entire workforce, including shop floor operators, is apprised of common social engineering tactics, therefore, is often an organization’s first – and possibly most important – line of defense.

*A data recovery plan can mitigate the risk*

Since manufacturers can scarcely afford network disruption, especially when it tampers with production and other physical systems, they would do well to invest in data recovery. On-site backups are helpful for immediate recovery, but off-site backups in a secure location add another layer of security. Recovery solutions are essential for restoring data and systems. It might also be worth investing in disaster recovery solutions to restore overall operations in the event of a major cyberattack.

**The promise and risk of innovation**

Manufacturers stand to gain a lot from digital transformation, but they must be aware of the cyber threats, taking care to prioritize security as they digitize. The lack of interoperability can lure manufacturers into the trap of deploying cybersecurity in segments, but they would benefit from taking a more comprehensive approach. Innovations can introduce new risks, but they’re always worth pursuing so long as you plan for those risks.