Manufacturing

Top 4 Cybersecurity Threats

The cybersecurity threats manufacturers should prioritize now.

splunk>

Foreword

Manufacturers have become resilience experts. Over the last few years, they have successfully bobbed and weaved through an onslaught of supply chain challenges, labor constraints, inflation pressures, and shifting regulatory requirements.

And whether by design or destiny, the industry has largely found itself in a better position. As we tally manufacturing's milestones, the rapid cloud and digital transformations of the early 2020s will likely rank somewhere alongside Henry Ford's moving assembly line in 1913 and the advent of industrial robots in 1954.

That's why I'm so confident in this industry's ability to not just navigate an evolving cyber threat landscape, but to harness it to fuel a smarter, more efficient manufacturing future.

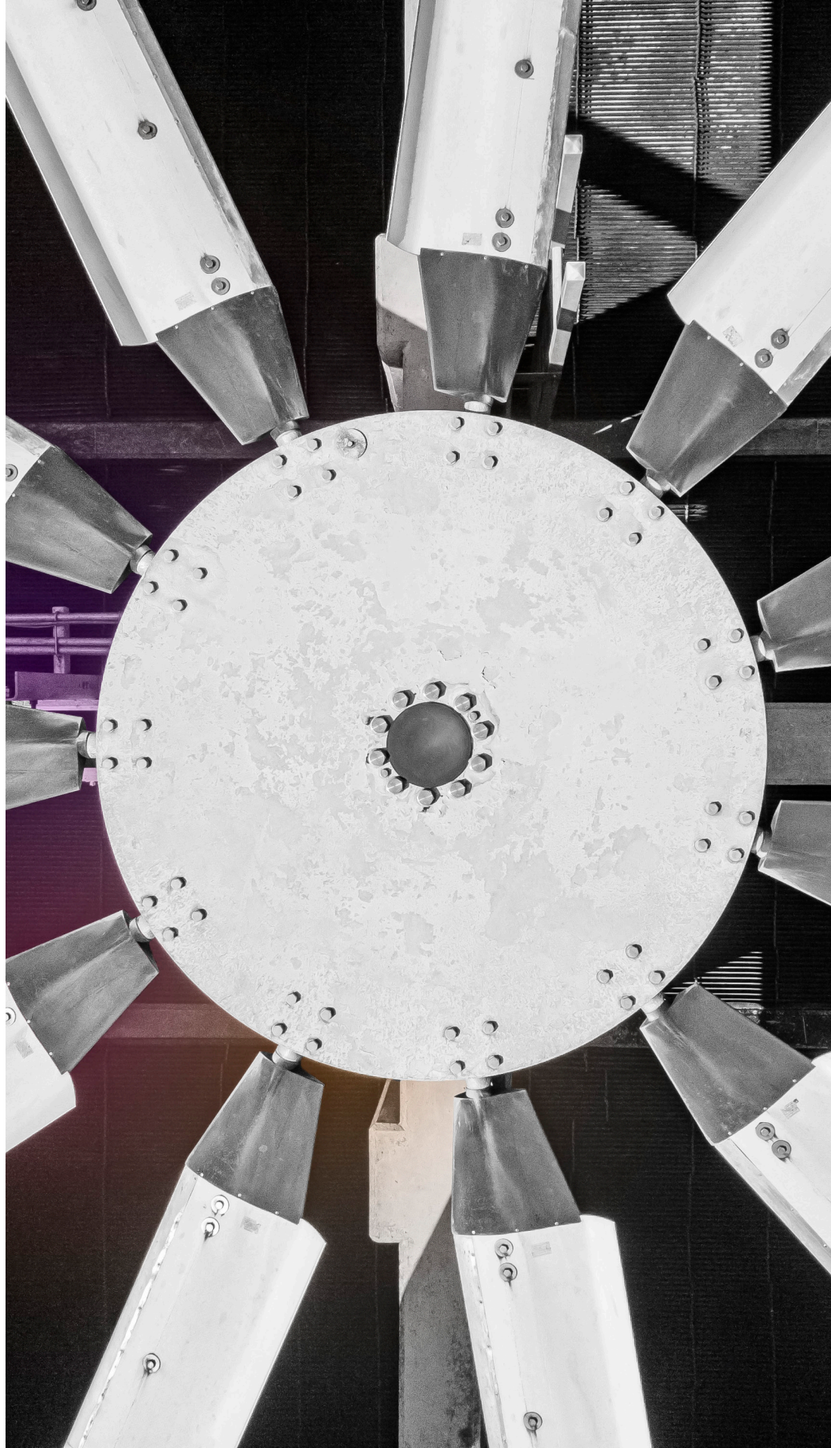
The stakes are high, and the bad actors are savvy. New weapons and attack portals pop up daily. In the dark corners of manufacturing's IT/OT networks, bad actors have gotten creative. And rich.

Manufacturers need a bright light. They need visibility into the hard-to-see corners of their networks, and a method for responding fast and at scale to increasingly pervasive cyberattacks.

And because there is nothing more unifying than a shared enemy, Splunk's Threat Research Team has identified and broken down the manufacturing industry's four highest-risk cyberthreats. We hope these insights can be a tool to break down silos, increase visibility and boost resilience in every corner of your manufacturing organization.

- Ewald Munz

Splunk Head of Manufacturing, Automotive and Sustainability EMEA



The state of cybersecurity in manufacturing

Today, the manufacturing industry claims the dubious honor of being the industry most targeted by cyberattack criminals. Since 2019, cyberattacks against supply chains have doubled. Just last year, attacks increased by more than 200%. And nearly half (49%) of manufacturing organizations suffered a data breach over the last two years, up from 39% the year before, according to Splunk's State of Security 2023 research.

According to the research, manufacturing security teams are being stretched toward a breaking point. Fifty-six percent say they don't have enough people to handle the increasing volume of security events (versus 47% across other industries), based on Splunk's research. More than half (51%) say they are considering a new job due to their current workload.

Three factors increase a manufacturer's attack surface area and threat risk:

Deep digital connectivity

Poorly secured OT on the factory floor is increasingly connected to IT in the enterprise, and most critically, the organization's valuable network of suppliers, retail partners and direct consumers. This ever-widening impact zone makes the industry a prime target for bad actors seeking more bang for their hacking buck.

Poor visibility

Silos between IT and OT obscure sightlines, and limit the reach of enterprise security into a growing catalog of point solutions on the factory floor. The evolution to hybrid, multicloud infrastructure threatens to further compound complexity and reduce visibility, just as interconnected supply chain networks and direct-to-consumer sales increase the industry's threat vortices.

Low tolerance for downtime

While nearly every other industry can maintain some degree of its business-critical operations during and following a cyberattack, bad actors can bring a manufacturing organization to a grinding halt. The State of Security 2023 revealed that the likelihood of a security incident shutting down business-critical systems in manufacturing is 44%, compared to 19% in other industries, spurring faster and higher ransom payouts.

Based on the work of Splunk's Threat Research Team, the following section breaks down the four top threats manufacturing leaders should prioritize now to make their factories more secure.

Threat 1

Ransomware

With an 83% year-over-year increase in ransomware attacks in the first three quarters of 2023, every industry should be building its defenses against ransomware.

Yet, manufacturing earned the unenviable top spot as the industry most impacted by ransomware in 2023, a ranking that has cost the sector an estimated $46 billion in downtime alone since 2018.

On average, companies paid out a jaw-dropping $1.54 million per ransomware attack in 2023, marking a steep raise for bad actors who averaged just $147,000 per attack in 2019.

A continued rise in direct-to-consumer (D2C) operations could push up payouts even more and solidify manufacturing's position as a popular ransomware target. Direct-to-consumer sales accounted for one in every seven ecommerce dollars spent in 2022, with a projected compound annual growth rate of 23% through 2023.

What you need to know

The manufacturing industry absorbed nearly a quarter (24.8%) of all industrial ransomware attacks in 2022. In such an attack, an infected host encrypts a victim's data, holding it hostage until they pay the attacker a fee. In recent ransomware attacks, hackers have threatened to leak or sell stolen data, exponentially increasing the damage potential.

Manufacturing is uniquely and inherently susceptible to ransomware attacks. Bad actors can literally turn off a factory's lights, shutting down assembly lines until a ransom is paid. Post-attack, each minute that passes racks up downtime costs, disrupts supply chains and inflicts reputational damage. High stakes and compounding costs prompt manufacturing organizations to pay higher ransoms than companies in other sectors, and to do so quickly.

Higher payouts and the fact that manufacturers rarely operate in a closed system make them a prime target. Interdependencies — between components suppliers, third-party logistics, distribution or retail partners — widen the industry's threat landscape and generate innumerable security gaps.

When a ransomware attack struck a global provider of instruments and services for the manufacturing industry in February 2023, the company's quarterly revenue dropped 20%, and it announced more than $200 million in Q1 losses alone. Downstream, a chip maker subsequently announced $250 million in losses related to a ransomware incident that hit one of its suppliers.

$1.54 million

On average, companies paid out a jaw-dropping $1.54 million per ransomware attack in 2023.

How the attack happens

In manufacturing, most attacks are deployed in IT on the corporate side — usually through spear-phishing campaigns, drive-by downloads and traditional remote service-based exploitation — and are designed to propagate to the OT side of the business.

About 90% of manufacturers have limited visibility into their OT systems and are otherwise poorly defended with weak network perimeters (90%), external connectivity exposure in their OT systems (80%) and shared credentials that make it easier for ransomware groups to infiltrate systems (60%).

Once it reaches the concrete environment, malware infiltrates legacy equipment and systems — many of which are unpatched and unsecured — and prompts users with a pop-up, or directs them to a website, where they're informed that their files are encrypted and can be released, for a fee.

Threat 2

Phishing

Phishing skirts technology and targets human beings, making it easy and profitable for bad actors.

Why? Because humans are fallible. Last year, human error accounted for 74% of data breaches.

And for manufacturers expanding into D2C operations and digital production lines, the number of humans who digitally touch their systems is on the rise.

Consumers and supply chain partners: In England and Wales, more than half of consumer phishing targets reported their attackers posed as delivery companies.

Employees: Web apps, including those used by remote workers, were responsible for 90% of data breaches in 2021.

As manufacturing companies extend digital access to a growing network of humans, tools and processes, they need reinforcements to protect their critical assets.

What you need to know

Manufacturers orchestrate a uniquely interdependent network of suppliers, distributors and customers. And those dependencies create shockwaves — when one manufacturer is attacked, other companies along their value and supply chains can be negatively impacted, even if they weren't directly targeted.

The world's third-largest aluminum producer closed many of its plants and moved others offline after attackers used credentials stolen in an earlier phishing attack in March 2019. The shutdowns, which cost the aluminum-maker $75 million, left its extensive network of aluminum-reliant manufacturers in a lurch. Manual operations during a nearly month-long shutdown kept product flowing but could have significantly impacted the downstream production of everything from toys to national defense vehicles.

While most manufacturers report confidence in the security of their own systems, they're wisely concerned about the people coming into their high-contact systems. Across email, websites and D2C portals, manufacturers face challenges in managing trust, validating entry points and stopping malicious code from sneaking through.

How the attack happens

A phishing attack tricks manufacturing customers, partners or employees into providing personally identifiable information, such as passwords and banking account details. Via email, victims might be directed to a highly convincing — but completely bogus — site designed to solicit and harvest information. Or they might be sent a link or an attachment that, once opened, launches a ransomware virus into every unsecured corner of your operation.

In January 2016, an employee at an aerospace parts manufacturing company received an email, purportedly from the organization's CEO, requesting a €43 million deposit into a dubious account as part of an "acquisition project." The money was never recovered.

While better training could help prevent attacks like this, more sophisticated phishing campaigns are harder to train for. A growing shift toward IT/OT convergence will force manufacturers to extend their defenses as their operations — and the sophistication levels of phishing threats — evolve.

Threat 3

Supply chain attack

Prior to February 2022, a mid-size manufacturer of cup holders, USB sockets and door pockets for car interiors, was little known outside of Japan — until its supply chain attack brought the world's top-selling carmaker to a screeching halt.

The carmaker had to halt its just-in-time production on 28 lines at 14 factories as it inspected and recovered its systems.

$375 million

All in, the supply chain attack cost the carmaker about $375 million and delayed production of more than 13,000 vehicles.

What you need to know

The major carmaker wasn't the only victim. As a third-party vendor to dozens of global manufacturing organizations, the attack was custom-designed to infiltrate the supplier's customer network. A trickledown of ransom demands and shutdowns at other major auto manufacturing companies generated incalculable damages.

As manufacturers continuously expand the scope and scale of their interconnected, global networks, supply chain attacks are dominating the threat landscape. Led by sophisticated hackers — often nation-state sponsored — in pursuit of big payouts, the number of supply chain attacks are expected to continue growing exponentially.

How the attack happens

Supply chain attacks often start with hackers targeting a single entity in the hopes of accessing information from that organization's customers.

Using legitimate, trusted processes, attackers gain full access to an organization's data by targeting the vendor's software source code, updates or build processes. Compromised vendors then inadvertently transmit malware to their customer network.

Supply chain attacks are difficult to detect because they happen at an offset to the attack surface. Breaches can reach victims through third-party software updates, application installers and malware on connected devices. One software update can infect thousands of organizations, with minimal effort from the hacker, who now has "legitimate" access to move laterally across thousands of organizations.

Threat 4

IoT threats

Thanks in large part to the manufacturing industry, the number of IoT-connected devices is expected to grow to 29 billion globally by 2030. IoT-powered predictive maintenance, quality control and inventory management are the tip of a smart factory iceberg transforming manufacturing processes today.

Those transformations will fuel more efficiency, improved safety and higher value. However, they also fueled a 77% increase in malware attacks on IoT-connected devices in 2022.

To maximize the upsides of IoT on the factory floor, manufacturers must reckon with increased risk.

What you need to know

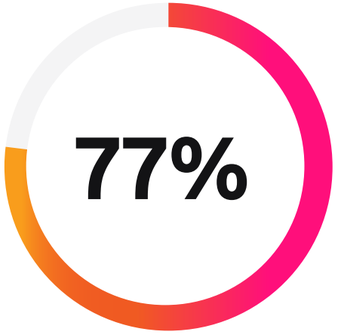
Manufacturers are getting smart with IoT, using cloud-connected devices to help automate the creation and delivery of products and the maintenance of machinery. In a smart factory, previously disparate systems and devices become connected so the stream of data they produce can be turned into actionable insight.

For good reason, manufacturing leaders are bullish in their assessment of IoT's potential: 67% of companies in the industrial manufacturing sector have an ongoing smart factory initiative.

However, those same systems can be used to shut your production line down.

Or worse.

In one extreme example, the well-known IoT attack, Stuxnet, used a worm to access top industrial program logic controllers at a uranium enrichment plant in Iran. The worm was able to damage 30% of the plant's centrifuges.



Manufacturers reported a 77% increase in malware attacks on IoT-connected devices in 2022.

How the attack happens

Hackers and malicious nation-states exploit vulnerabilities in connected IoT devices with sophisticated malware. Once inside your network, they can monitor users and steal intellectual property, classified or personally identifying data, and other critical information.

Once they infiltrate an IoT system, hackers can also use their newly gained access to move into other connected devices or to gain entry to your enterprise network.

Building digital resilience with edge to enterprise visibility.

Cyberattacks are inevitable in manufacturing. However, a unified platform designed to drive faster detection, investigation and response can help manufacturers build digital resilience.

With Splunk, manufacturers can gain comprehensive visibility across digital systems and respond faster to security threats, keep operations up and running, integrate IT and OT systems, and unlock innovation.

Splunk helps manufacturers:

Prevent major issues

Splunk provides comprehensive visibility over an organization's digital systems, which helps surface key risks and detect incidents before they become major issues.

Remediate faster

Issues that threaten the supply chain are inevitable, so it is critical to prioritize incidents and standardize workflows so that when incidents do occur, organizations can minimize outages and breaches and resume operations quickly.

Adapt to new opportunities

Digitally resilient organizations will be able to secure and seamlessly integrate IT, OT and IoT data, and even harness untapped data that lives on the edge. By removing security and IT complexity, engineers can free up their time spent on responding to issues so that they can build new tools and processes that will improve their customer experiences and operational excellence.

Discover how Splunk can help your manufacturing organization gain comprehensive visibility across digital systems to respond faster to evolving security threats, keep operations up and running, integrate IT and OT systems, and unlock future-ready resilience.

Learn more

24.ebook.manufacturings top 4 cybersecurity threats.r4

www.splunk.com/manufacturing

splunk>