BITSIGHT

WHITE PAPER

Building Better Visibility into Manufacturing Cybersecurity Programs

Introduction

As manufacturers invest in smart factories and autonomous operations, factory floors and product lines become more connected than ever. Emerging technologies in these areas will support new lines of revenue and leaps in operational efficiency for manufacturers. However, manufacturers must also be aware of the new risks that come with these gains. While many manufacturers already have IT-focused programs that provide visibility and controls over their business network infrastructure, the capabilities of this cybersecurity infrastructure rarely provides cover beyond back office tech functions.

Limitations in visibility into cyber exposures beyond that traditional bubble will make it difficult for manufacturers to understand where cyber risks exist across supply chains, operational technology on the factory floor, and within connected customer devices, let alone work on controlling them.

Here's what manufacturing leadership needs to know about why they should start retooling risk strategies to build a modern manufacturing cybersecurity program, along with what it takes to broaden cyber risk visibility across the supply chain, operational technology, and customer environments.

Digital Resilience is The Key to Manufacturing Success

Smart factories and digital transformation are key to long-term competitiveness and profitability in manufacturing. By embedding digital technologies into factory processes and establishing more connectivity into the factory floor—and the products themselves—manufacturers stand to improve:

- Safety and sustainability
- Asset efficiency
- Product quality
- Cost efficiency
- Workforce efficiency

According to a recent Deloitte study, 83% of manufacturers today believe that smart factory solutions—technologies like AI, 5G, Internet of Things, data analytics, and cloud computing—stand to transform the way products are made in the next five years.[1]

Rapid adoption of emerging technology in manufacturing doesn't just bolster factory efficiency. It also opens up a whole new world of revenue generation. One of the most promising examples of this comes in the form of product servitization, where aftermarket service is made possible by IoT connectivity built into a manufacturer's products. Recent studies show that 71% of industrial companies today look positively on the prospect of aftermarket services.[2] And analysts estimate that while manufacturers make just over 10% of their revenue through digital services, that percentage will reach 29% by 2030.[3]

All of this digital progress opens up new opportunities, but it also opens up new opportunities to cyber attackers. Added connectivity in devices on the factory floor, with supplier systems, and in new products creates new attack surfaces that manufacturers have to monitor and manage.

[1] *https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook.html*

[2] *https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook.html*

[3] *https://www.gartner.com/en/documents/4487599*

Not to mention the reality that the resilience of the digital services is now vital to the business.

Ten years ago, a cyber attack against business systems would still cost a manufacturer considerable expense, but it would rarely threaten core production systems. Now, cyber attacks on manufacturers frequently impact critical factory systems and the consequences are no longer just regulatory fines or breach expense, but also existential threats to business viability.

Now, cyber attacks on manufacturers frequently impact critical factory systems and the consequences are no longer just regulatory fines or breach expense, but also existential threats to business viability.

Manufacturing Digital Trends That Impact Cyber Exposure

Product servitization

Industrial Internet of Things (IIoT) proliferation

IT/OT convergence

Convergence of software & manufacturing supply chain

Manufacturing Cyber Risk Landscape

Like any enterprise, manufacturers face all of the same risks of cyber attacks against their IT infrastructure that a typical business would in other verticals. They're called to protect a range of traditional business systems, IT networks, and hybrid cloud infrastructure. But that's just the tip of the cyber risk iceberg for manufacturers.

In addition to these traditional cybersecurity pressures against their IT assets, manufacturers must also manage cyber risks that threaten the factory floor and the supply chains that keep their production lines running. As factory equipment, logistics, and even the manufactured products themselves grow increasingly digitized and connected, operational technology (OT) cybersecurity risks are mounting for manufacturers.

With so much exposure on so many levels, it's no surprise that the cybercriminals are gravitating toward manufacturers. According to a recent study, manufacturing has topped the list of industries suffering cyberattacks for three years running. Sadly, 85% of those incidents could have been mitigated with patching, multi-factor authentication, or by adhering to least privilege principles.

The manufacturing space needs better cybersecurity visibility and controls to manage the following cyber risks that jeopardize the reliability and safety of their industrial infrastructure.

CIA or AIC

As in many other verticals, manufacturers must task their cybersecurity teams with ensuring the confidentiality, integrity, and availability of their information and assets across their tech infrastructure. However, in the industrialized world of manufacturing, the order of priority for CIA is inverted. Manufacturers seek to protect AIC, where availability is most important, followed by integrity, and then confidentiality.

BLENDED IT-OT THREATS

OT has traditionally been considered a separate entity from IT networks, but digital transformation has blurred the lines between OT and IT networks. OT and industrial control system (ICS) assets are increasingly internet connected to enable more efficient factory operations, while industrial internet of things (IIoT) telemetry has rapidly proliferated to support everything from better preventative maintenance to smarter inventory management. Meantime, rogue and loosely sanctioned IT devices making their way on to OT networks are contributing to a growing shadow OT problem that is increasing the size of this risk surface.

A recent study by Bitsight security researchers shed some light on the vast scale of this growing attack surface against manufacturers and other critical infrastructure companies facing this IT-OT convergence problem. The research found nearly 100,000 industrial control assets owned by organizations around the world that were exposed to the public internet. These are crucial OT systems that control critical OT processes—including those that keep factories running.

COMPLEX SUPPLY CHAIN CYBER RISKS

Manufacturers are no strangers to managing supply chain risks. Establishing strong vendor relations to ensure the reliability, quality, and logistics around the raw materials and equipment necessary to build products has long been a manufacturing core competency. What's changing is that there are now a myriad of layered cyber risks that also must be accounted for to maintain a robust physical and digital supply chain.

The cybersecurity posture and resilience of their manufacturing suppliers—whether they're providing raw materials, equipment, or digital services—now has the potential to make or break whether a manufacturer is able to keep its production lines running.

Vulnerabilities and breaches in these suppliers' environments could threaten their ability to reliably provide goods and materials that could threaten manufacturing downtime and add costs to the equation. As such, cybersecurity visibility is now a crucial tool for manufacturing supply chain management.

What's more, manufacturers are often called to embed connected digital components from their suppliers directly into their products. Similarly, they also closely partner with suppliers, integrating their software and platforms with these third parties and leveraging supplier portals and platforms to order products and interact with their contacts at these vendors. Vulnerabilities in these supplier components and attacks against their underlying platforms quite frequently expose the manufacturers to new attack surfaces that can threaten the security and resilience of the manufacturer's factories and product lines.

PRODUCT SECURITY IN THE AGE OF IOT AND SERVITIZATION

Manufacturers are leveraging the increasing connectivity in the products they produce to roll out a ton of new aftermarket services to their customer environments. Many visionaries in the manufacturing world see this shift toward servitization—essentially diversifying revenue streams from a product-oriented model to a service-oriented model—as a way for manufacturers to supercharge their revenue streams. One particularly bullish estimate said that the global everything as a service (XaaS) market, spurred on in large part by manufacturing-led servitization, will crack $1.2 trillion in revenue by 2030.[4]

All of that added revenue comes with heavier responsibility from manufacturers. As manufacturers ship connected products that they maintain, communicate with, and update over time, product security no longer ends at the customer's doorstep. With IoT connectivity and servitization, product security now has to be an ongoing concern. Attacks against customers through the manufacturer's connectivity and service platforms could be devastating to its brand and customer relationships. Attacks against these connected products could also potentially threaten the viability of the service if an attacker uses those exposures to get deeper in to the manufacturer's software infrastructure and digital networks. Additionally, this burgeoning area of exposure also increases regulatory and legal risks to manufacturers if they don't properly address the issue.

RANSOMWARE

Manufacturing is becoming one of the most targeted industries for ransomware criminals who understand that manufacturers can't afford the downtime and are perfect targets for cyber extortion.

Recent studies show that 65% of manufacturers today have been hit by ransomware in the past year—a marked increase of 41% since 2020. Each of these attacks cost manufacturers a mean of $1.67M to recover from–whether they paid a ransom or not. In most instances manufacturers are so debilitated by these attacks that they end up just paying the ransom. Research shows six in ten manufacturers today pay to get their data back or otherwise meet criminal extortionist demands. In the cases where manufacturers feel their best chance of recovery is making a ransom payout, the median payment is $1.2 million–but there are clearly many that pay much more than that as the mean is $2.36 million.

REGULATORY RISKS

As the attacks intensify, so too does regulatory scrutiny of manufacturing cybersecurity practices. Manufacturing organizations must comply with an increasingly complex tapestry of cybersecurity regulations. Some of the heavy hitters that have arisen in recent years include the new SEC cybersecurity rules that require transparency about material cybersecurity incidents and the Cybersecurity Maturity Model Certification (CMMC) program, which governs both OT and IT security standards for US Department of Defense vendors. Additionally, emerging standards like IEC 62443 are growing in prominence for manufacturers and other industrials, prescribing stronger ICS/OT security controls in critical infrastructure.

While some regulations focus on the entire manufacturing organization, others zero in on the security of the manufactured products themselves, introducing cybersecurity as a prerequisite for market access. NIS2, for instance, ensures that manufacturers—among other sectors—implement comprehensive cybersecurity measures. On the other hand, the Cyber Resilience Act (CRA) and UNECE Regulation 155 exemplify product-focused regulations. Starting in 2027, the CRA will prevent the sale of products with digital elements—such as connected toys, home security cameras, and solar panels—in the EU if they lack adequate cybersecurity protections. In the automotive industry, vehicles produced after July 2024 must comply with UNECE Regulation 155 to obtain the necessary certification for market entry.

Many of these regulations, such as NIS2 and UNECE 155, also emphasize the critical role of supply chain security. They require companies to address cybersecurity risks not only within their own operations but also throughout their supply chains and supplier relationships, underscoring the interconnected nature of today's manufacturing landscape.

Manufacturers must also be tuned to regulations around consumer and citizen protections—such as GDPR—which govern how technologies like IoT are used and how they handle data when embedded in manufactured products.

[4] *https://www.the-future-of-commerce.com/2023/02/08/servitization-in-manufacturing-new-services-drive-growth/*

[5] *https://news.sophos.com/en-us/2024/05/28/the-state-of-ransomware-in-manufacturing-and-production-2024/*

4 Visibility Keys to Cyber Risk Management in Manufacturing

In order to effectively address the threats emerging from this risk landscape, manufacturers need to invest in a holistic cybersecurity program that's attuned to the full range of IT and OT concerns. Establishing visibility starts with a manufacturer's own blended IT-OT infrastructure, but organizations will also need to account for complex supply chain and product security risks. The following are four keys to achieving the kind of visibility manufacturers need to effectively manage risks as they embrace manufacturing 4.0.

1 GETTING THE BASICS OF IT VISIBILITY LOCKED DOWN

Certain cyber monitoring and risk management practices are universal across all industries, and manufacturing is no different. Before a manufacturer tackles the nuances of OT cybersecurity, it will need to build a foundation of strong IT visibility and control first. The following are three core components to tackling the basics of IT visibility that manufacturers will need to help them start to future-proof their insight into blended IT-OT threats and cyber supply chain risks.

External Attack Surface Management

Some 76% of organizations today have experienced at least one cyber incident due to the exploitation of unknown or unmanaged assets.[6] External attack surface management (EASM) tools provide the ability to not only discover assets and catalog them, but also offer contextual information about potential exposures within these assets. The best EASM tooling provides visibility across a range of assets, including previously unknown SaaS, cloud, and third-party assets.

Third Party Risk Management

With so many manufacturing supply chain vendors conducting business over connected platforms, and increasingly more supply chain vendors integrating their software into factory equipment and components used in the production process, manufacturers need clarity about the security issues these connections and dependencies expose them to. This is why cybersecurity third-party risk management (TPRM) is such a crucial discipline of vendor management for manufacturers today. Unfortunately, many manufacturers don't have visibility in place to track third-party exposure. KPMG reports that just 41% of manufacturers take a risk-based monitoring approach to TPRM.[7]

Cyber Risk Quantification

Manufacturing executives need to understand the financial risk of cybersecurity consequences much in the same way that they can quantify the risk of downtime to their factory equipment when it breaks down. Cyber risk quantification (CRQ) programs calculate risk exposure and the potential financial impact of these exposures. In order to get any degree of accuracy, CRQ needs to be backed by a foundation of knowledge about assets, the value of the processes they support and the exposures impacting those assets that are at highest risk of being exploited. EASM and security performance management platforms can prove crucial to these efforts.

Manufacturing executives need to understand the financial risk of cybersecurity consequences much in the same way that they can quantify the risk of downtime to their factory equipment when it breaks down.

[6] https://www.techtarget.com/searchsecurity/opinion/Why-companies-need-attack-surface-management-in-2024#:~:text=The%20research%20also%20indicated%20that,and%20change%20isn't%20easy.

[7] https://kpmg.com/xx/en/home/insights/2020/12/industrial-manufacturers-struggling-with-tprm-programs.html

2 OUTSIDE-IN OT VISIBILITY INTO CYBER THREATS TO MANUFACTURING FLOOR

Getting visibility into threats to OT assets and the environment is a tricky prospect. Manufacturers can't actively scan industrial control systems in the same way that they would an IT system or network. Just the act of looking into these systems can cause system instability that will cost a manufacturer extensive downtime costs. A simple ping sweep will overwhelm some ICS assets and cause system instability that may result in extensive downtime costs. And because many ICS assets aren't based on general purpose operating systems, run on outdated versions of operating systems such as Windows NT, or can't sacrifice immediate response over the latency imposed security software or firmware, agent software can't be installed. Similarly, critical manufacturing operational equipment has less appetite for the risks of disruption that can come from patching.

There are very niche industrial cybersecurity products that provide an inside-out view of ICS systems by extracting data from the ICS historian—sometimes referred to as 'passive scanning' by some OT security firms. These views are crucial for manufacturers but limited to ICS systems and take significant investment and expertise to support and to integrate into broader IT cybersecurity programs.

For manufacturers that are still maturing their security program, EASM offers a manageable place to start before jumping into these niche monitoring products. Using EASM to discover OT assets exposed to the internet can provide visibility into the places where rogue IT connections or other breaks in the Purdue model occur.

Meantime, for manufacturers that already do use ICS-centric security products, layering in EASM provides more telemetry and points of visibility to manufacturing environments. This can extend visibility into some of the manufacturing IIoT devices that these products may not track as comprehensively.

What is the Purdue Model?

The Purdue Model is a hierarchical model that segments IT and OT network design into six functional levels, from Level 0 to Level 5. The model defines the barriers and controls around connections between the layers.

3 CYBER RISK AWARENESS ACROSS MANUFACTURING SUPPLY CHAINS

Manufacturers need TPRM and Vendor Risk Management visibility to improve manufacturing supply chain resilience. Most crucially, manufacturers need visibility into TPRM risks that span across blended OT-IT environments and that are layered into every part of the supply chain, whether it's from raw material suppliers, delivery logistics firms, or equipment suppliers. For example, if a supplier has connectivity into a manufacturer's digital ecosystem with access to OT infrastructure SCADA workstations that control OT systems, they could be adding risk to the OT environment.

Additionally, because many manufacturers are themselves part of other manufacturers' supply chains, these organizations will want to think about how they can facilitate relationships with their customers to provide the cybersecurity visibility that they'll demand for their own TPRM and supply chain security efforts.

4 BOLSTERING PRODUCT SECURITY IN CUSTOMER ENVIRONMENTS

As products are increasingly digitized, software security has become a crucial part of the comprehensive product management and product security function. Manufacturers must be prepared to bolster application security from design, to test, to pushing embedded software live within their products. They'll also be called to secure the connection and security of devices out in customer environments when they're running the manufacturer's services and platforms.

This can be especially challenging for hardware and other goods manufacturers that may not have a pedigree in software design and defensive software development. Many such manufacturers may have very mature product safety and quality control processes in place, but could still be in the earliest stages of building out their application security (AppSec) program. A refrigerator manufacturer, for example, may need to think differently about software protections needed once their new IoT module is included in units.

This will take significant investments in new AppSec and security operational processes, in which both EASM and Security Performance Management can play a role. These technologies should be tuned for visibility into both operations and product security, especially to support that range of secure aftermarket services that are enabled through IoT connectivity.

EASM will not solve all of these product security issues, but the security operational support it provides can help supplement work done by the AppSec team in prioritizing work to find and remediate the riskiest flaws in product-facing software, including risks in external code dependencies and misconfigurations.

How Bitsight Empowers Better Program Visibility

Manufacturers need strong cybersecurity practices backed by visibility into digital risks that span across IT and OT networks.

Bitsight invented the security ratings industry in 2011, and in the process of refining its ratings platform the company created a methodology for examining exposure that was essentially a frontrunner for exposure management visibility. The truth is that Bitsight has been enabling customers to manage their external attack surface and reduce exposures since the earliest iterations of the Bitsight platform. Today, Bitsight's research team constantly collects data from over 120 threat sources to power its exposure management tooling.

Bitsight's Security Performance Management platform performs automated and continuous asset and vulnerability discovery across a range of endpoints, servers, cloud instances, certificates, IoT devices, operational technology (OT) assets, and mobile apps. It's also on the hunt for other active threats and exposures that includes compromised assets, botnets, domain squatting, compromised credentials, misconfigurations, and dark web activity around assets.

One of the big differentiators Bitsight offers over competitors in the exposure management market is its Third-Party Risk Management offering, which extends exposure visibility out across the IT supply chain. That's one of the reasons why KuppingerCole rates Bitsight as an Overall Leader, Product Leader, and Market Leader in the 2023 Leadership Compass for Attack Surface Management report.

See How Bitsight Can Help

Request your custom attack surface report and gain better visibility of your manufacturing cybersecurity program

Get Your Report →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE

BITSIGHT