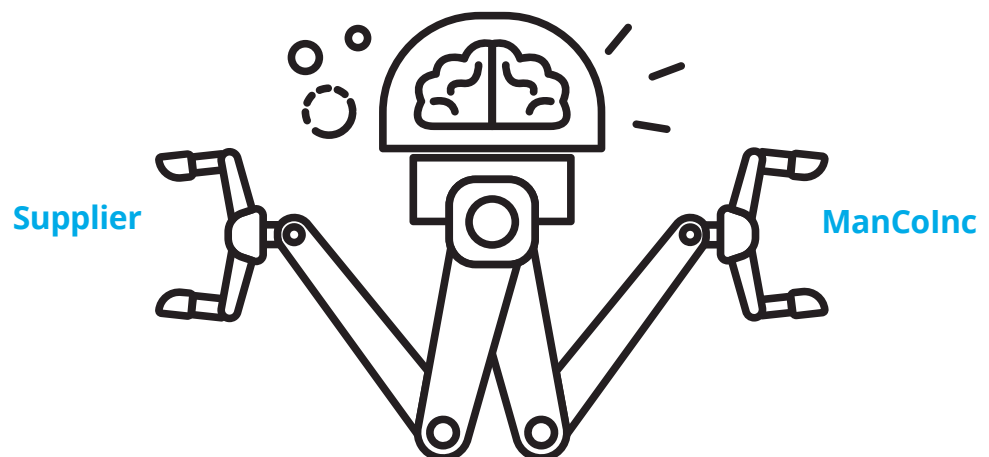




It is 2025. ManCoInc,¹ an industrial manufacturer, operates through 20 connected and smart manufacturing facilities around the globe. The company is also connected digitally to its suppliers and customers. One day, a key supplier suffers a cyberattack. The malicious code enters the supplier's system of record, causing production to shut down temporarily. The code then attempts to propagate to all partners that are connected to that supplier. ManCoInc, however, has a mature cybersecurity program in place that is able to detect, isolate, and block the code from infecting its network. Which outcome would you prefer: that of the supplier, or that of ManCoInc?



Introduction

The newest chapter in industrial development, commonly known as the Fourth Industrial Revolution, heralds an era of tremendous potential for innovation and growth. It also brings with it new risks and challenges. Nowhere might this be more apparent than in the manufacturing cyber landscape. The rise of digital technologies and global interconnectivity marks a new level of complexity. Cyber is no longer limited to certain aspects of operations or certain people; rather, it is everywhere, likely in places manufacturing leaders haven't considered. Every employee, every partner, every electronic device, piece of machinery, or finished product brings with it the potential for cyber risk. And many manufacturers could be underprepared for its potential impact.

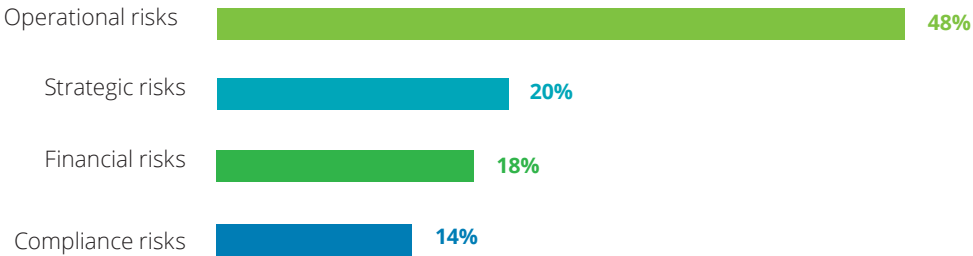
Deloitte and the Manufacturers Alliance for Productivity and Innovation (MAPI) have been formally studying cybersecurity and associated risks since 2016. Our joint studies have found that while awareness of the potential cyber threats related to smart factory initiatives are growing, many manufacturers have had difficulties advancing their cyber risk management capabilities. The 2016 Cyber Risk in Advanced Manufacturing Study identified that one in two manufacturers surveyed were only "somewhat confident" with their preparedness to address cyber threats.² In the 2019 Deloitte and MAPI Smart Factory Study, we found that one in four manufacturers surveyed have not performed a cyber risk assessment in the past year, which means these manufacturers likely do not have visibility to the impact a cyberattack could have on their organization's operations.³

The 2019 Deloitte and MAPI Smart Factory Study revealed a number of risks relative to smart factory initiatives, spanning enterprise categories from operational to financial and strategic to compliance (figure 1)⁴. Forty-eight percent of manufacturers surveyed identified operational risks, which include cybersecurity, as the greatest danger to smart factory initiatives. With the interconnectedness of smart factory technologies, cyber threats are among the most prevalent, as smart factory environments expose people, technology, physical processes, and intellectual property to these risks.

Complicating adoption of smart factory technologies is the reality that management of information technology (IT) is often out of sync with operational technology (OT) management, which can further expose companies to cyberattacks resulting from unknown or underappreciated vulnerabilities.⁵ The adversaries often execute attacks through the use of malware, and the results can be devastating: Several recent notable attacks have affected manufacturing operations and cost companies \$150 million or more. In one case, the attack even affected safety systems, increasing the risk of harm to humans.



Figure 1. The primary risks related to smart factory initiatives

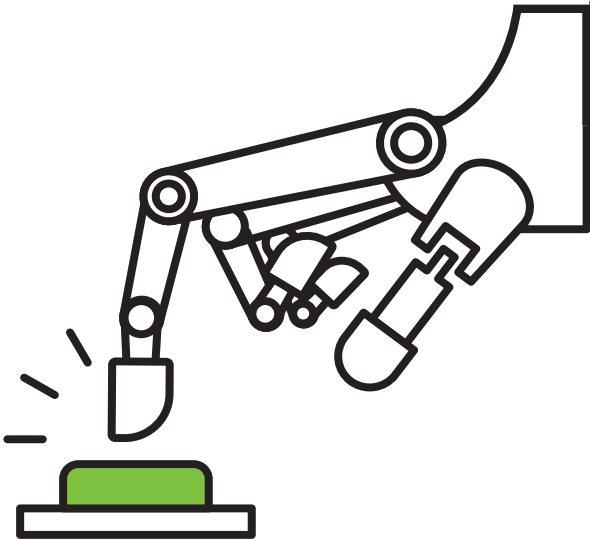


Source: 2019 Deloitte and MAPI Smart Factory Study

The current risk landscape seems to raise some key questions:

- To what extent are cyber threats affecting manufacturers today?
- What type and level of risks exist in present-day factories?
- How do manufacturers address today’s cybersecurity risks? And how will they address new risks?
- How do manufacturers build cybersecurity controls into their smart factory initiatives?

This report addresses the above questions and presents a closer look at the risk profiles of six of the most active smart factory use cases the 2019 Deloitte and MAPI Smart Factory Study identified. Armed with this information, manufacturers can make informed decisions to better manage cyber risk as part of a broader strategy to manage operational risk.



Growing cyber threats can be a menace in manufacturing environments

Cyber threats: By the numbers

The 2019 Deloitte and MAPI Smart Factory Study identified that more than 8 in 10 manufacturers surveyed have at least some capabilities to detect and respond to cyber threats.⁶

However, industry-wide cyber-related incident data suggests this may be overstated (figure 2).

Figure 2. Cyber-related manufacturing incidents

4 in 10 manufacturers

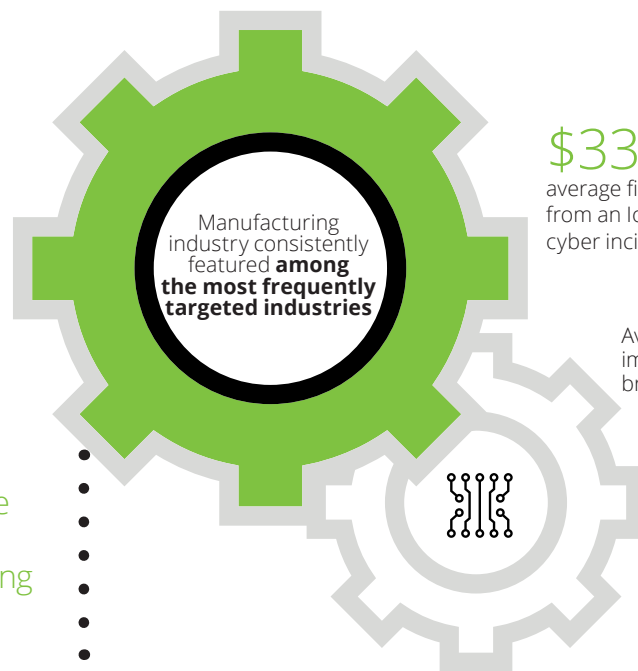
surveyed indicated that their operations were affected by a cyber incident in the past 12 months



Between 2017 and 2018, cyber incidents increased by:



3.5x Ransomware
2.5x Spoofing
0.7x Spear-phishing



\$330,000

average financial impact from an IoT-focused cyber incident



Average financial impact from a data breach in 2018

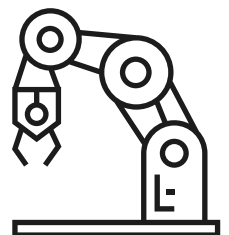
\$7.5M



87%
Unauthorized access

86%
Operational disruption

85%
Intellectual property theft



Source: Multiple news articles and press releases ^{7,8,9,10,11,12,13,14}

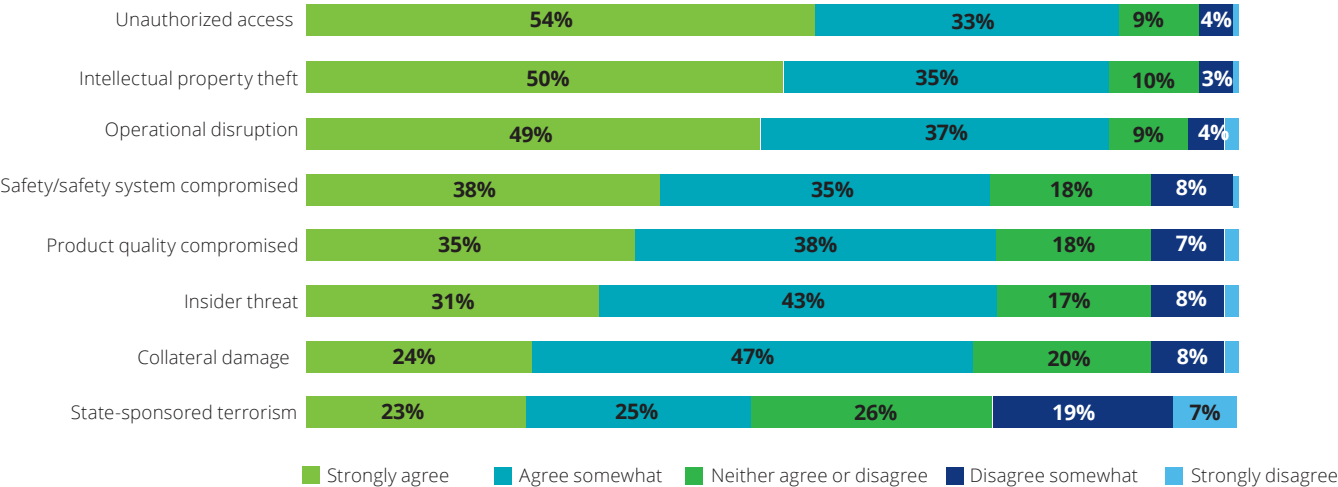
Behind the numbers: A proliferation of threats

Many manufacturing companies are seeing an increase in cyber-related incidents associated with the control systems used to manage industrial operations. These systems can range from programmable logic controllers and distributed control systems to embedded systems; special-purpose systems; industrial IoT devices; those systems that manage quality; health, and safety; and even the building or facility management systems. Collectively, these control systems make up the operational technologies that allow facilities to operate.

Today, these OT systems are being integrated with advanced technologies such as sensors and aggregation platforms. These systems now have the ability to remotely track and control production in real time, plan resources, and diagnose and minimize production errors. The number and variety of employees that have access to these connected OT systems has expanded beyond the shop floor to include vendors, suppliers, and business users, who are often spread across factories and geographies.

While the advantages of connectivity include increased levels of productivity, faster identification and remediation of quality defects, and better collaboration across functional areas, they can also multiply the potential vulnerabilities of the smart factory. In fact, the Cybersecurity and Infrastructure Security Agency lists 1,200+ known OT system-related security issues, vulnerabilities, and exploits from more than 300 OEMs and system providers.¹⁵ These cyber issues can interrupt operations or compromise safety. The methods include denial-of-service attacks or adversaries using administrative privileges to execute new code. In short, the threat landscape for the systems that control operations of a production facility has proliferated rapidly with the increase in digitization and advanced technologies. The 2019 Deloitte and MAPI Smart Factory Study identified that manufacturers seem most concerned with risks related to unauthorized access, intellectual property theft, and operational disruption (figure 3).

Figure 3. Cyber risks in the OT environment



N=209 (Q19-Q32) What risk(s) are you concerned about in your OT environment? For the following potential risks, rate from a scale of 1 to 5, with 1= "strongly disagree that we are concerned" to 5 = "strongly agree that we are concerned"

Source: 2019 Deloitte and MAPI Smart Factory Study

The root cause: IT and OT are out of sync

To gain operational efficiency and assure better customer service, many manufacturing companies are looking to converge IT and OT across their operations. As figure 4 suggests, there are many areas where people, process, and technology overlap between the IT and OT ecosystems—areas where respective strategies need to be in sync. The reality of these technologies and how they are used, however, is often markedly different. OT system-related investment decisions are often made on the factory floor by leaders within operations, with less involvement from corporate

IT and security departments. This can lead to a myriad of different technologies, often with different security control capabilities, that will likely need to be integrated to and then managed using existing IT network infrastructures. The convergence of IT and OT security can be a challenging task, since routine IT procedures, such as antivirus software updates or even patching, can lead to significant production disruptions, even potentially shutting down entire production lines.

Figure 4. Operational technology ecosystem driving cyber concerns

OT system characteristics	Cyber concerns
The complexity of IT and OT convergence	<ul style="list-style-type: none"> • OT is typically managed by engineering, automation, and operations rather than IT. • There is generally no single team responsible for all OT systems and underlying security. • Traditional application of security controls such as patching or vulnerability scanning cannot usually occur without detailed evaluation due to potential effects. • Deep knowledge of the industrial processes, technology assets, network architectures, risks, and security approaches are often essential, leading to the need for integrated teams across both IT and OT working together.
Update paradox	<ul style="list-style-type: none"> • Traditional application of security controls such as patching or vulnerability scanning cannot usually occur without detailed evaluation due to potential effects. • No single approach for patching or updating systems is possible. This can make it difficult to be responsive when vulnerabilities are detected, often driving the need for defense-in-depth approaches to be adopted.
Legacy system setbacks	<ul style="list-style-type: none"> • Many systems have long life cycles (10+ years) and were not built to be externally connected. With the increase in edge computing, cloud platforms, and the adoption of other smart factory technologies, air gapping is no longer a viable option.
Destabilized infrastructure	<ul style="list-style-type: none"> • Older equipment often uses proprietary communication protocols that can be easily disrupted if data communication within the network segments increases. • Existing networks and associated architectures were not designed to handle the data flows required for the adoption of these new technologies. • There are limited vetting processes to understand the security risks associated with new technologies being acquired and deployed—increasing the risk of an attack affecting both this new technology and other legacy technologies on the same networks.
Operational constraints	<ul style="list-style-type: none"> • Real-time capabilities are typically essential; introducing additional security controls could introduce latency. • Making network or other changes could require downtime or an outage. Downtime due to maintenance should be limited to absolute minimums. • Software updates are often not possible due to the proprietary nature of products or contracts or equipment age. • Establishment of clear responsibilities across functions (IT and OT) can be crucial. It is important to approach addressing cybersecurity risks using cross-functional teams, considering what each group does well.

Today's IT departments are often being tasked with managing security for these heterogeneous OT environments and coordinating the new generation of operational technologies alongside existing IT-managed systems, such as enterprise resource planning (ERP) packages. Our recent Smart Factory Survey reveals that IT leaders surveyed were more confident than their OT counterparts (detecting threats 41 percent for IT vs. 33 percent for OT; responding 34 percent for IT vs. 29 percent for OT)—indicating a gap between the two groups in having visibility to the risk profile of the organization.

Aspects of security can be overlooked when implementing advanced technologies and smart factory initiatives. Ongoing OT system security is not typically covered in the service-level agreements and contracts with system integrators and equipment vendors. Even when covered, these contracts rarely include statements for maintaining security controls, which by default makes it the responsibility of the business process owners. As a result, some large capital projects may omit any budget for ongoing security management of OT systems that could critically affect operations if they were targeted by an attack.



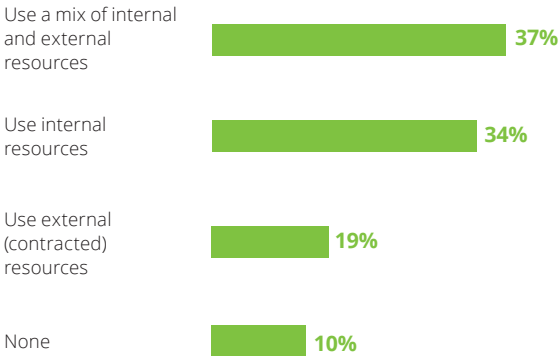
Confidence in cyber detection may create a false sense of security

Adding advanced technologies to OT networks requires equally sophisticated cybersecurity standards. A significant share of manufacturers, however, have yet to build the cyber capabilities to secure some of these business-critical systems. Given the rapid pace at which new technologies are added to factories via smart factory use cases, IT and OT leaders may be unprepared to respond to new threats that arise. While 90 percent of manufacturers surveyed in the study report capabilities to detect cyber events, very few companies today have extended monitoring into their OT environments, and fewer than half of manufacturers surveyed have performed cybersecurity assessments within the past six months (figure 5).¹⁶ Additionally, it could often prove difficult to identify an attack if it originates within the OT environments unless there is a negative effect on operations (because monitoring capabilities have not been extended).

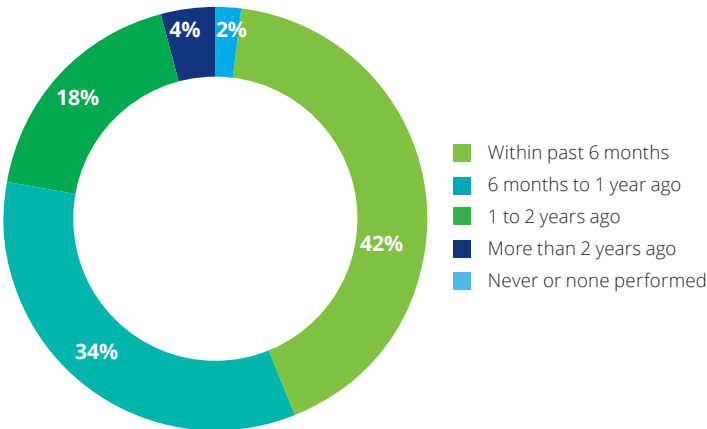
These responses indicate that surveyed manufacturers seem more confident in their cyber preparedness than the maturity and capabilities they may have to respond to and recover from a cyberattack, especially when new technologies come online in periods between risk assessments. It is likely that some manufacturers are not aware of the new threats they face when leveraging IoT devices and other emerging technologies in a smart factory environment. Even if they know that something bad could happen, often they do not understand how.

Figure 5. Capabilities to detect cyber events vs. recent cybersecurity assessments

Capabilities to detect cyber events



Most recent cyber risk maturity assessment



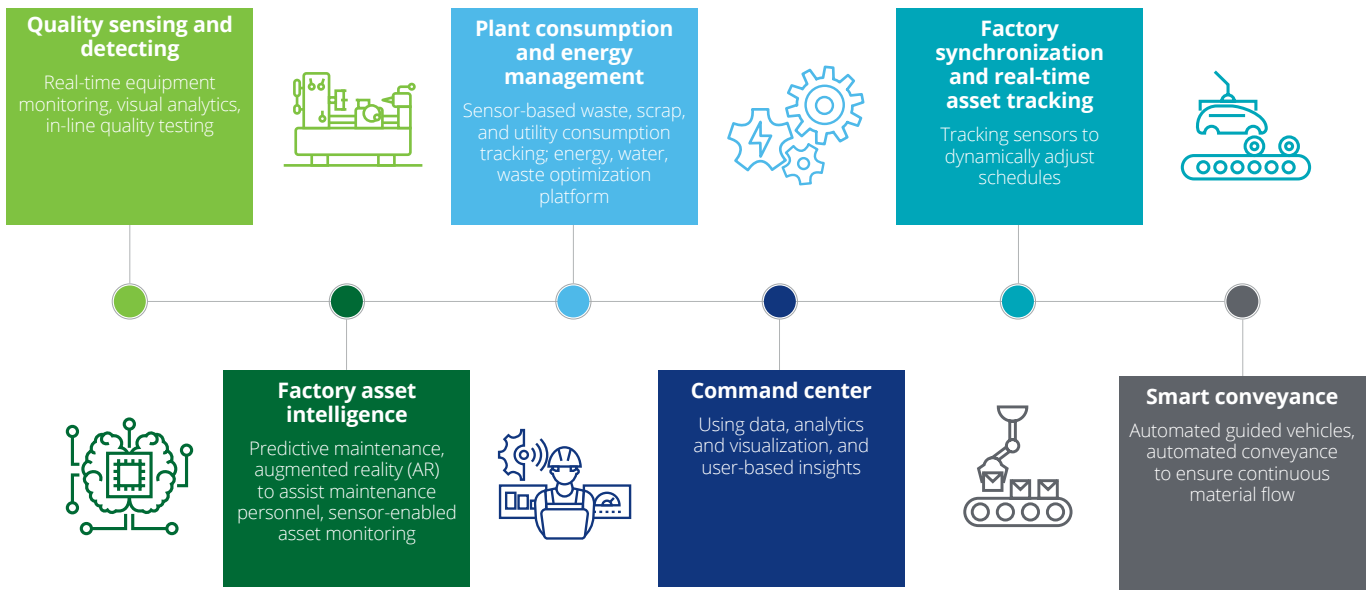
Source: 2019 Deloitte and MAPI Smart Factory Study

Decoding cyber risk through smart factory use cases

Smart factory initiatives are commonly approached from a use-case perspective, in which advanced technologies are combined with process innovation to address a specific business challenge or opportunity. For example, quality sensing and error detecting is a use case that incorporates vision systems, edge computing, and artificial intelligence (AI)-based analytics to reduce defect rates on a production line.

One way manufacturers can understand the cyber risks that smart factory initiatives could introduce is through these use cases. Identifying the data types and owners, along with the entry point(s), can help to clarify threats and vulnerabilities. Below, we highlight six use cases (figure 6).

Figure 6. Six smart factory use cases



Source: Deloitte analysis of the 2019 Deloitte and MAPI Smart Factory Study data

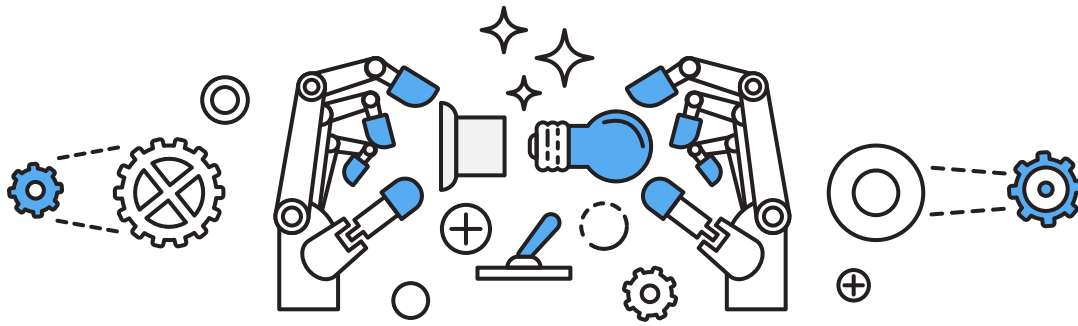


Figure 7. Cybersecurity considerations for six smart factory use cases







1 Engineering collaboration/digital twin-enabled product design

Capability		Virtual models of a physical product (or assembly) to run simulations, predict product performance, and make iterative design modifications
Data types		Product configurations, materials, other intellectual property (IP), customer usage data, repair and warranty data, quality data
Data owners		Engineering and design department, product management, after-market service, quality control, suppliers
Entry points		Hardware including AR glasses, laptops, VR caves; software applications, databases, and analytics tools; network and cloud
Threats/vulnerabilities		Network-enabled engineering software could be accessed by others with access to that software. Hardware (e.g., AR glasses) could be taken by someone and used to view sensitive product or customer data. The data uploaded to a cloud platform for analysis and simulation could be compromised.
Cybersecurity considerations		<ul style="list-style-type: none"> Restrict device and system access to authorized personnel only and follow a least-privilege approach. Ensure cloud access and storage follows access control protocols—confirm that secure network architectures are applied to control system and data connections. Apply defense-in-depth strategies: Detect, plot, and translate the cyber threat landscape. Use threat intelligence specific to OT environments with a monitoring capability that can identify abnormal behavior. Develop a documented response plan for a cyberattack that could affect physical processes or one that results in a data breach.







2 Risk-adjusted material requirement planning (MRP)

Capability		MRP involves estimating the required volume of materials at the respective locations at the right time. Risk-adjusted MRP makes use of both production and demand data-driven insights and stochastic algorithms to optimize the flow of materials in a manufacturing process.
Data types		Bills of material, customer order/demand data, planning data (routing, labor, machine availability, quality standards, scrap percentages), supplier information
Data owners		Procurement department, production department, supplier network
Entry points		Company intranet, software programs, data that resides at suppliers
Threats/vulnerabilities		Risks of phishing and cyberattacks can cause data loss and system failures. Data compromise could affect material replenishment or delay production.
Cybersecurity considerations		<ul style="list-style-type: none"> Control and manage access of users to systems and from one system to another system. This includes identity and access management, remote access, and privileged access management. Define company-wide policy for secure remote access, managing connectivity for both employees and third parties. Establish or join trusted exchange centers that are focused on sharing cyber intelligence. Use simulations like wargames and tabletops to rehearse responses. Build muscle memory in employees around how to react/respond to phishing attempts (e.g., through establishing phishing campaigns). NOTE: Email and Internet access should not be allowed within OT environments. If required, such connectivity should be tightly controlled and monitored. Instead, this type of access should be restricted to business networks where possible.







3 Advanced manufacturing

Capability		Technologies such as additive manufacturing (3D printing) with advanced materials for parts/assemblies and for prototyping
Data types		CAD/CAM files, material-specific data, material requirements, 3D printer specifications
Data owners		Production department, engineering and design team, procurement
Entry points		Shop floor
Threats/vulnerabilities		A cyberattack could result in confidential product composition or design-related data loss, as well as bring down a production line or facility through access to the networked 3D printer(s).
Cybersecurity considerations		<ul style="list-style-type: none"> Protect critical infrastructure and OT network to defend the processes, communications, and assets. Confirm that 3D printers are appropriately segmented within the network. Perform cyber compromise assessments, security evaluations of new technologies, and threat modeling and simulation exercises. Develop a process to provide timely notification and response to cyber incident. A focus should be on confirming an organization's ability to restore operations to normal state quickly—this includes backing up systems and configurations.







4 Robotics and cognitive process automation

Capability		Robotic process automation (RPA), machine learning, natural language processing, and AI. These technologies can automate repetitive and time-intensive tasks, especially on the production floor.
Data types		Performance data, rules-based data, data captured from computer vision, asset data
Data owners		Production department, data analytics team, robotics team
Entry points		HMI (human-machine interface), robotic arms, software programs
Threats/vulnerabilities		Unauthorized access, unwarranted bot programs, and denial-of-service attacks that could lead to disruption of a production line
Cybersecurity considerations		<ul style="list-style-type: none"> Employ application whitelisting, source code review, and file integrity monitoring to minimize the risk of malicious code being installed and executed. Correlate internal events with external threat intelligence to enhance organization's capabilities and tailor risk responses in alignment with criticality and likelihood. Confirm there is an accurate inventory of all technology assets, along with a process for assessing potential business impact.

5 Factory asset intelligence and performance management

Capability		Predictive maintenance, AR to assist maintenance personnel, sensor-enabled asset monitoring
Data types		Machine-specific performance data, OEE data, maintenance scheduling and repair history
Data owners		Operations and production team; maintenance and repair team
Entry points		Assets on production lines; maintenance staff and third parties
Threats/vulnerabilities		Access to OT environment via software that may have been developed without considering security needs. AR glasses could be compromised. Cyberattackers could gain visibility to factory asset data, including product and client information, or could disrupt production and damage assets.
Cybersecurity considerations		<ul style="list-style-type: none"> Adopt a risk-based approach rather than compliance-based approach. Approach security considering defense-in-depth needs with a consistent program and structure—educating personnel, gaining visibility across the sites, segmenting the network, monitoring for abnormal behavior, and having a capability to respond/recover. Continuously assess entry points, motivation, and vehicles to execute an attack to enable the organization's technical teams to build operational response capabilities. Perform simulation exercises and workshops to stress-test existing plans in a controlled environment. Involvement of key personnel across departments should be considered during these simulations, from the analysts with hands on the keyboard to the executives who would have ultimate decision-making power.

6 Plant consumption and energy management

Capability		Sensor-based waste, scrap, and utility consumption tracking; energy, water, and waste optimization platform
Data types		Facility-related for climate control, energy usage, factory asset energy consumption
Data owners		Facility management, operations
Entry points		HMI, building control systems, asset-based software
Threats/vulnerabilities		Unauthorized access could lead to disruptions in energy flow to the plant, damaging equipment and materials while also having the potential to injure people.
Cybersecurity considerations		<ul style="list-style-type: none"> Patch and update these systems where it is possible. A robust vulnerability management and patching program is needed. Continuously assess entry points and detect malicious activities through 24x7 monitoring of environments. Activity monitoring should occur in a central location and be extended across both IT and OT. Responsibilities for key contacts should be assigned across manufacturing plants to personnel who will provide support when research or triage is required. Create cross-disciplinary playbooks to manage communications and actions during an incident. These playbooks should cover both IT and OT and be updated based on lessons learned (i.e., through testing activities and responding to actual events).

Next steps: Where to start building cyber resilience in the smart factory

As smart factory initiatives continue to proliferate across the global footprint of manufacturers, cyber risks are expected to continue to increase. As the 2019 Deloitte and MAPI Smart Factory Study reveals, the cyber preparedness of many manufacturers is less mature than likely necessary to protect against not only current threats, but also new threats and vulnerabilities that digital technologies create. Manufacturing organizations should invest in a holistic cyber management program that extends across the enterprise (IT and OT) to identify, protect, respond to and recover from cyberattacks. Specifically, the following four steps should be considered when starting the process of building an effective manufacturing cybersecurity program:

- 1. Perform a cybersecurity maturity assessment.** If your organization has not done this in the past year, consider making this a priority, as with every new use case in pilot or production within the smart factory, there come new exposures to threats. The assessment should include OT environments; business networks; and advanced manufacturing cyber risks such as IP protection, control systems, connected products, and third-party risks related to industrial ecosystem relationships (for example, vendors, suppliers, or partners).
- 2. Establish a formal cybersecurity governance program that considers OT.** The program should provide consistency and roll out to manufacturing locations globally. Business-centric representation in these governance structures is important to allow IT and OT teams to collaborate where practical and manage the business. The manufacturing security teams should work closely with the site to consider the risks and appropriate mitigation strategies. Consider using a steering committee to assign decision-making authority to further deliver consistency within the program.
- 3. Prioritize actions based on risk profiles.** Use the results of the cybersecurity maturity assessment to create a strategy and roadmap that can be shared with executive leadership and, where appropriate, the board to address risks that are commensurate with your organization's risk tolerance and capabilities. It is important to understand your manufacturing environments and the assets that comprise them so tailored mitigating controls can be designed and implemented.
- 4. Build in security.** Since many smart factory use cases are still in planning and early stages, now is the time to harmonize these projects with your cyber risk program. Design and include the appropriate security controls at the front end of these projects. Important controls to consider include use of secure network segmentation models, deployment of passive monitoring solutions (to provide visibility of networked assets and activity while minimizing the risk of disruption), secure remote access, control of removable media, improved management of privileged access, and executing consistent backup processes (especially for critical systems and configurations).

The breadth and depth of potential threats and vulnerabilities in a connected smart factory environment remind us of the reality that cyber risk is everywhere today. Strong cybersecurity is the foundation for a resilient company. This requires that all employees are front-line defenders of your organization's security. Make sure your employees are aware of their responsibilities, and give them tools to be cyber-resilient citizens. With effective cyber risk management for smart factory initiatives, manufacturers can capitalize on the upside potential the Fourth Industrial Revolution brings and prevent themselves from becoming a victim of a future cyberattack.

Endnotes

1. ManColnc is a hypothetical company for illustrative purposes.
2. Ibid.
3. Deloitte, *2019 Deloitte and MAPI Smart Factory Study*.
4. Ibid.
5. Deloitte, "Cyber risk in advanced manufacturing: Getting ahead of cyber risk," 2016, <https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html>.
6. Deloitte, *2019 Deloitte and MAPI Smart Factory Study*.
7. IoT Business News, "New 2019 Global Survey: IoT-Focused Cyberattacks are the New Normal," May 29, 2019, <https://iotbusinessnews.com/2019/05/29/94747-new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal>.
8. Infosec, "Which Industries Are The Biggest Security Targets?," <https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-threats-by-industry/#gref>.
9. Ethan Bresnahan, "Carbon Black Report Indicates Industries Most Targeted for Cyber Attack, Security Boulevard, April 2, 2019, <https://securityboulevard.com/2019/04/carbon-black-report-indicates-industries-most-targeted-for-cyber-attack>.
10. Deloitte, "Cyber risk in advanced manufacturing."
11. Gregory Garrett, "Cyberattacks Skyrocketed in 2018. Are You Ready for 2019?," IndustryWeek, <https://www.industryweek.com/technology-and-iiot/cyberattacks-skyrocketed-2018-are-you-ready-2019>.
12. IoT Business News, "IoT-Focused Cyberattacks are the New Normal."
13. Garrett, "Cyberattacks Skyrocketed in 2018."
14. Deloitte, *2019 Deloitte and MAPI Smart Factory Study*.
15. US Cybersecurity and Infrastructure Security Agency, "ICS-CERT Advisories," <https://www.us-cert.gov/ics/advisories>.
16. Deloitte, *2019 Deloitte and MAPI Smart Factory Study*.

Authors

Ramsey Hajj

Advisory Principal
Deloitte & Touche LLP
+1 561 962 7843
rhajj@deloitte.com

Sean Peasley

Advisory Partner
Deloitte & Touche LLP
+1 714 334 6600
speasley@deloitte.com

Jason Hunt

Advisory Senior Manager
Deloitte & Touche LLP
+1 901 322 6804
jashunt@deloitte.com

Heather Ashton Manolian

US Industrial Products & Construction
Research Leader
Deloitte Services LP
+1 617 437 2120
hashtonmanolian@deloitte.com

David Beckoff

VP, Product Development & Insights
MAPI
+1 703 647 5153
dbeckoff@mapi.net

**About Deloitte**

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

About MAPI

Founded in 1933, the Manufacturers Alliance for Productivity and Innovation is a nonprofit organization that connects manufacturing leaders with the ideas they need to make smarter decisions. As the manufacturing leadership network, its mission is to build strong leadership within manufacturing to drive the growth, profitability, and stature of global manufacturers. For more information, visit mapi.net.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.