KPMG

Cyber considerations for Industrial manufacturing in 2024

kpmg.com

Foreword

The industrial manufacturing sector is undergoing a major transformation, driven by the convergence of digital technologies, such as the Internet of Things, artificial intelligence, and cloud computing. This convergence is creating new opportunities for manufacturers to improve efficiency, productivity, and agility. However, it is also creating new cybersecurity risks.

Industrial manufacturing companies are finding themselves increasingly exposed to cyber risks, including in their interdependent supply chains, threats to resiliency, and complex global regulatory requirements. Addressing these expanded cyber risks and complying with an ever-increasing spectrum of regulations are key challenges for this sector.

Many organizations' current approach to third-party and supply chain security does not align with the reality of today's complex and interdependent ecosystem of partner organizations. Organizations must establish more strategic supplier partnerships focused on continuously monitoring and managing the evolving risk profiles of these suppliers to strengthen operational resilience.

Industrial manufacturers need to be able to calibrate their regulatory reporting for an increasingly borderless world but also maintain security controls tailored to local requirements. Organizations should be prepared to respond quickly to changing regulations and requirements.

During a cyber incident, organizations must respond rapidly to detect, contain, eradicate, and recover despite an increasingly challenging global business landscape and regulatory environment. In today's volatile environment, resilience has become a common theme for organizations across the industrial manufacturing sector, with executives focused on resilience and recovery across key organizational systems if preventative controls fail.

This report explores cybersecurity considerations for the industrial manufacturing sector. It provides an overview of the rapidly evolving cybersecurity landscape, calls for increasingly sophisticated compliance monitoring and controls, and explores enhancements to operational resilience.

Michael Gomez
Lead Principal, Strategy and Governance
Cyber Security Services
KPMG LLP

Cyber considerations 2024

Key Cybersecurity considerations for Industrial manufacturing companies in 2024

1

Navigate blurring global boundaries

2

Modernize supply chain security

3

Align cybersecurity with organizational resilience

1

Consideration: Navigate blurring global boundaries

Global businesses are operating within an increasingly complex cyber and privacy regulatory space. National interests are playing out, leading to diverse regulatory requirements over information sovereignty, supply chain security, transparency of cyber controls compliance, and incident reporting. Businesses should seek to calibrate their regulatory reporting for an increasingly borderless world but also maintain security controls that can be tailored to local requirements. Organizations should be prepared to respond quickly to changing requirements.

Key challenges

Common goals but disjointed regulatory landscape – The global regulatory landscape is beginning to coalesce around common regulatory patterns and approaches, but significant differences still exist across regions and markets for cybersecurity, privacy, and (AI) regulations. Organizations must carefully manage data sovereignty requirements to ensure compliance.

Data sovereignty laws dictate how and where data can be collected, stored, and processed, varying significantly from country to country. For example, the US International Traffic in Arms Regulations stipulates requirements for access to controlled technologies (e.g., technologies with military applications). The European Union (EU) has strict requirements for the transfer of personal data outside of the EU. China, India, and many other countries have similar laws restricting the flow of data across borders.[1]

Shifting global dynamics influencing response speed and adaptability – With a wide range of approaches to data regulation (including differing definitions of personal data, governance frameworks, and accountability rules), navigating incident detection, response, and business continuity is an increasingly complex undertaking for global businesses.

Industrial manufacturing businesses must navigate detecting and investigating incidents as well as responding and recovery to ensure resiliency within the context of this complex regulatory environment.

Key opportunities

Harmonized cyber and data governance – As common patterns and approaches emerge in the global regulatory landscape, organizations can begin to develop harmonized frameworks to organize governance of cybersecurity, privacy, and AI, and meet global obligations.

Shift-left innovation – With technological advancement in industrial manufacturing, the "shift left" approach offers opportunities to embed security measures at the onset of solution design and service delivery.

Global collaboration – International conversations can improve collaboration in digital security, providing repeatable leading practices and enhancing interorganizational cooperation across various markets and regions.

[1]Source: The International Traffic in Arms Regulations (ITAR website): Article – DDTC Public Portal

2

Consideration: Modernize supply chain security

Many organizations' current approach to third-party and supply chain security does not align with the reality of today's complex and interdependent ecosystem of partner organizations. Traditional models were built around the assumption that third parties provide services on a transactional basis. That view does not reflect today's intricate network of application programming interfaces (APIs) and processes tethered by a complex set of software-as-a-service dependencies.

Organizations are encouraged to establish more strategic supplier partnerships focused on continuously monitoring and managing the evolving risk profiles of these suppliers to strengthen operational resilience.

Key challenges

Supply chain visibility – Large organizations can have thousands of suppliers, and often they cannot accurately assess their activities with traditional methods. It would require an army of security personnel to do all the physical endpoint assessments, which is humanly impossible. It would cost tens of millions of dollars, making it unrealistic logistically and financially.

Supply chain dependency – Cyber intruders often target software and hardware vulnerabilities, posing a significant threat to supply chains. The industrial manufacturing sector operates within a complex ecosystem that includes intricate information exchange through dynamic APIs. Security weakness in this ecosystem can create a massive ripple effect. Instances like the SolarWinds attack remind us of the far-reaching consequences of these dependencies.

Weakest link – Industrial manufacturing firms often share sensitive information with business partners, exposing them to data leakages and/or cyberattacks through these links. The strength of cybersecurity measures is dependent on the weakest link in the chain, underlining the crucial yet challenging task of conducting thorough third-party due diligence.

Regulatory consequences – Many industrial manufacturing firms work with a complex array of suppliers to deliver products and services and some regulations require that organizational suppliers meet the same or similar cybersecurity requirements to the primary organization.

Key opportunities

Supply chain integration – Integrating cyber considerations into engineering and procurement processes presents a huge opportunity for organizations to minimize risks emerging from supply chain compromises. This proactive approach can strengthen enterprise positioning.

Regulatory awareness – Ensuring that all suppliers meet contractual and regulatory requirements via assessments, control testing, and reporting requirements will ensure that an organization does not run afoul of its supply chain regulatory requirements and help to avoid fines, penalties, and loss of business.

Supplier risk management – Continual monitoring and inventory assessment of frequently used suppliers and/or software can help organizations better understand providers' security structures and identify potential risks. Sharing information can enhance supply chain relationships and solidify leading practices.

Intelligent automation – Improving ongoing visibility into changing supplier risk profiles can help build a sustainable and scalable forward-looking third-party program.

Crowdsourcing intelligence – Encouraging the crowdsourcing of intelligence within your organization and with trusted third parties can provide collective cybersecurity insights, enhancing threat detection and response capabilities.

With increased instances of supply chain disruptions, industrial manufacturers investing in comprehensive risk management need to have a clear, continuous view of an ever-expanding third-party ecosystem. With today's complex global dynamics, it is crucial to evolve toward a cybersecurity posture that encompasses businesses and the vendor ecosystem.

3

Consideration : Align cybersecurity with organizational resilience

During a cyber incident, organizations need a response measured in minutes and hours, not days and weeks. In today's volatile environment, resilience has become a common theme for organizations across the industrial manufacturing sector, with executives focused on resilience and recovery across key organizational systems if preventative controls fail.

Resilience should seamlessly align with cybersecurity, emphasizing protection, detection, and rapid response and recovery. Cyber resilience is vital for maintaining business operational capabilities, safeguarding customer trust, and reducing the impact of future attacks. These disciplines should work in tandem to help organizations manage risk.

Key challenges

Maintain trust following an incident – A cybersecurity incident can threaten the trust organizations must maintain with vital stakeholders, and thus harm operational resilience. Rebuilding trust can be about rapid technical recovery or identifying alternate ways of delivering services. It is critical to identify impacted stakeholders and expeditiously address their needs to minimize disruption.

Identify and protect critical assets – To respond effectively to an incident and facilitate efficient and effective recovery, organizations must know which assets are most critical to business processes and have enabled enhanced resiliency processes to safeguard these assets. Organizations can ensure their most critical assets are protected by engaging in business impact assessments to determine asset criticality and tabletop exercises to test response and recovery capabilities.

Outdated infrastructure contains cyber vulnerabilities – Many organizations in the industrial manufacturing sector rely on outdated software and manufacturing technologies. This can be due to the risks to operational resilience if they replace tools and processes that are currently in use to meet production goals. However, unpatched vulnerabilities can present significant cybersecurity risks and lead to cybersecurity incidents that compromise organizational resiliency.

Internet-of-Things and (IoT) Operational Technology (OT) are difficult to secure – IoT and OT technologies often utilize rare operating systems and feature niche environments. As a result, vulnerability scanning, patching, and incident response are more difficult when IoT/OT is used within an organization's networks.

Adapt to an evolving threat landscape – As cyber defenses improve, attackers are getting more sophisticated as well, changing the threat landscape. Organizations need to continually improve and adapt. Resilience means being better equipped to address an incident quickly, comprehensively, and with minimal business impact. It does not mean there will never be another incident. Chief information security officers cannot control external threats but can control an organization's preparedness.

Key opportunities

Build trust with rapid recovery and stakeholder engagement – Industrial manufacturers can build trust with key internal and external stakeholders by building resiliency into the culture with robust planning, testing, and management of response and recovery processes. This will help ensure rapid response and recovery and minimal business disruption.

Modernize infrastructure – Outdated infrastructure presents serious cybersecurity risks since end-of-life software cannot be patched by the manufacturer and thus open vulnerabilities will not be patched. Organizations should work to update any software or systems running software that is no longer supported by the manufacturer as quickly as possible.

Secure IoT/OT Infrastructure – Develop a strategic approach to securing IoT/OT environments, including identifying and engaging expert vendors, and establishing resiliency measures to ensure business continuity in the event of an incident involving IoT or OT technologies.

Conduct comprehensive risk management – It is critical for an organization to assess, understand, and evaluate the risks it faces to strategically prioritize cybersecurity investment and improve organizational resilience. This risk management should include Identifying asset criticality and enabling enhanced resiliency measures on an organization's most critical assets.

Real-world cybersecurity in the industrial manufacturing sector

Companies in the industrial manufacturing sector are increasingly facing cybersecurity and regulatory risks because of their extensive reliance on digital channels and global operations. Unauthorized network access can lead to substantial financial losses, reputational impacts, compliance penalties, legal action, and erosion of customer trust.

Example 1

A major defense contractor acquired a new business with operations across several countries, including the United States and the United Kingdom. This introduced challenging data sovereignty issues as the United States and the United Kingdom have data sovereignty laws limiting the flow of applicable data across borders. As a result, the company needed to adhere to complex data security requirements and identity management rules across multiple countries and environments.

To resolve these issues, KPMG is helping the company to carefully navigate global regulatory requirements and manage most operations within national borders. KPMG is building an identity and access management program to ensure that access to sensitive data elements is restricted to authorized individuals located within appropriate jurisdictions.

Example 2

A major manufacturer with extensive use of IoT/OT recently surfaced issues with its IoT/OT risk management, supplier risk management, incident detection and response, and vulnerability management. Vulnerability scanning, patching, and log management are all more difficult in IoT/OT environments due to rare operating systems and niche environments. Suppliers can also use insecure remote access methodologies. These challenges increase cybersecurity risks for IOT/OT components.

To remedy, KPMG helped the company to develop an IoT/OT strategy that included network segmentation to contain potential cyber incidents and reduce risk, network detection and response for rapid identification of potential cybersecurity incidents, and improved access controls, especially with respect to third-party vendor access to IOT/OT infrastructure.

Example 3

A major auto manufacturer struggled to manage supply chain security and experienced several supply chain incidents that impacted production and manufacturing of vehicles. The company lacked visibility into the security of its manufacturing suppliers.

To remedy, KPMG helped the company to develop a manufacturing cybersecurity supplier program. KPMG developed a framework for assessing suppliers to ensure adequate cybersecurity and led a pilot program with 30 onsite assessments for the most critical suppliers. KPMG also developed policies, standards, methodologies, and related tools such as residual risk assessment questionnaires.

Top priorities for industrial manufacturing security professionals

- Harmonize cyber and data governance to navigate a complex regulatory environment
- Collaborate globally to establish repeatable leading practices across countries and regions
- Integrate cybersecurity considerations into supply chain risk management to reduce risk
- Integrate risk management into all cybersecurity decisions, especially to identifying and managing supply chain, regulatory, and business continuity risks
- Modernize infrastructure to reduce risk of vulnerabilities and retire end-of-life technologies

As industrial manufacturing organizations lead the charge in implementing emerging technologies to modernize delivery of services and solutions, they must also be aware of the accompanying risks. By carefully navigating global regulatory requirements, integrating cyber considerations into supply chain risk management, establishing a comprehensive business continuity program, and modernizing essential infrastructure, industrial manufacturing companies can position themselves for successful management of key security risks.

How KPMG professionals can help

In addition to assessing your cybersecurity program and helping ensure it aligns with your business priorities, KPMG professionals can help industrial manufacturers develop advanced digital solutions, advise on the implementation and monitoring of ongoing risks, and help design the appropriate response to cyber incidents.

KPMG professionals are adept at applying innovative thinking to industrial manufacturing firms' most pressing cybersecurity needs and developing custom strategies that are fit for purpose. With technology that is secure and trusted, KPMG professionals offer a broad array of solutions, including cyber cloud assessments, privacy automation, third-party security optimization, AI security, managed detection, and response.

KPMG. Make the Difference.
Learn more at kpmg.com/cybersecurity

Contact us

Michael D. Gomez
Lead Principal, Strategy and Governance
Cyber Security Services
michaelgomez@kpmg.com

Ellen Ozderman
Managing Director, Advisory
Cyber Security Services
eozderman@kpmg.com

Gregory Ligon
Senior Associate, Advisory
Cyber Security Services
gligon@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**