WORLD
ECONOMIC
FORUM

Building a Culture of Cyber Resilience in Manufacturing

WHITE PAPER

MAY 2024

Images: Midjourney, Getty Images

Contents

Disclaimer

This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Executive summary

The manufacturing sector operates within a complex ecosystem, characterized by a variety of sites, extensive supply chains and interlinked networks. This ecosystem relies on a multitude of suppliers, vendors and partners.

Over the past decade, manufacturing has been experiencing a swift digital transformation, which is fuelling growth, efficiency and profitability. This trend has also exposed the sector to a wide range of cyberthreats, making it the most targeted by cyberattacks – over the past three years, the manufacturing sector has accounted for one in four of all cyber incidents.

At the 2023 Annual Meeting of the World Economic Forum in Davos, business leaders highlighted the need to address cybersecurity risks for manufacturing at the ecosystem level, thus kick-starting the Cyber Resilience in Manufacturing initiative. Led by the Centre for Cybersecurity and the Centre for Advanced Manufacturing and Supply Chains at the Forum, this initiative has brought together more than 30 representatives from across the manufacturing ecosystem. The aim is to develop actionable guidance on how to develop a culture of cyber resilience.

Through extensive research and consultations with industry leaders as well as standard-setting and regulatory bodies, the Cyber Resilience in Manufacturing initiative has previously underscored the five primary challenges for developing a culture of cyber resilience in the manufacturing ecosystem. In response to these, the initiative has also formulated three guiding principles to support manufacturing and supply chain leaders in establishing a pervasive strategy for developing a cyber resilience culture throughout their organizations:

1. **Make cyber resilience a business priority:** Embed cyber resilience in the organization’s DNA or foundational structure, from the leadership to the shop floor.

2. **Drive cyber resilience by design:** Integrate cybersecurity into people, processes and assets.

3. **Engage and manage the ecosystem:** Build trusted partnerships, manage third-party risks and raise security awareness by identifying the key stakeholders.

These three principles are interlinked and mutually supportive – and are applicable across any manufacturing industry and location. Each principle is defined with additional guidance, contextualized with key considerations and complemented with real-world manufacturing use cases to facilitate adoption and effective implementation.

The playbook suggested in this paper serves as a pragmatic framework to enable businesses to navigate strategic, organizational, operational, technical and regulatory challenges – and will foster a robust culture of cyber resilience that can effectively counteract both current and future threats.

1 Prioritizing cyber resilience in manufacturing

Manufacturing is among the sectors most targeted by cyberattacks, with disruptions having severe impact on the global economy.

1.1 Why cyber resilience is vital for manufacturing

Manufacturing is a global and diverse sector that is essential to society and the global economy. It spans various industries such as consumer goods, electronics, automotives, energy, healthcare, food and beverage, heavy industry, and oil and gas.

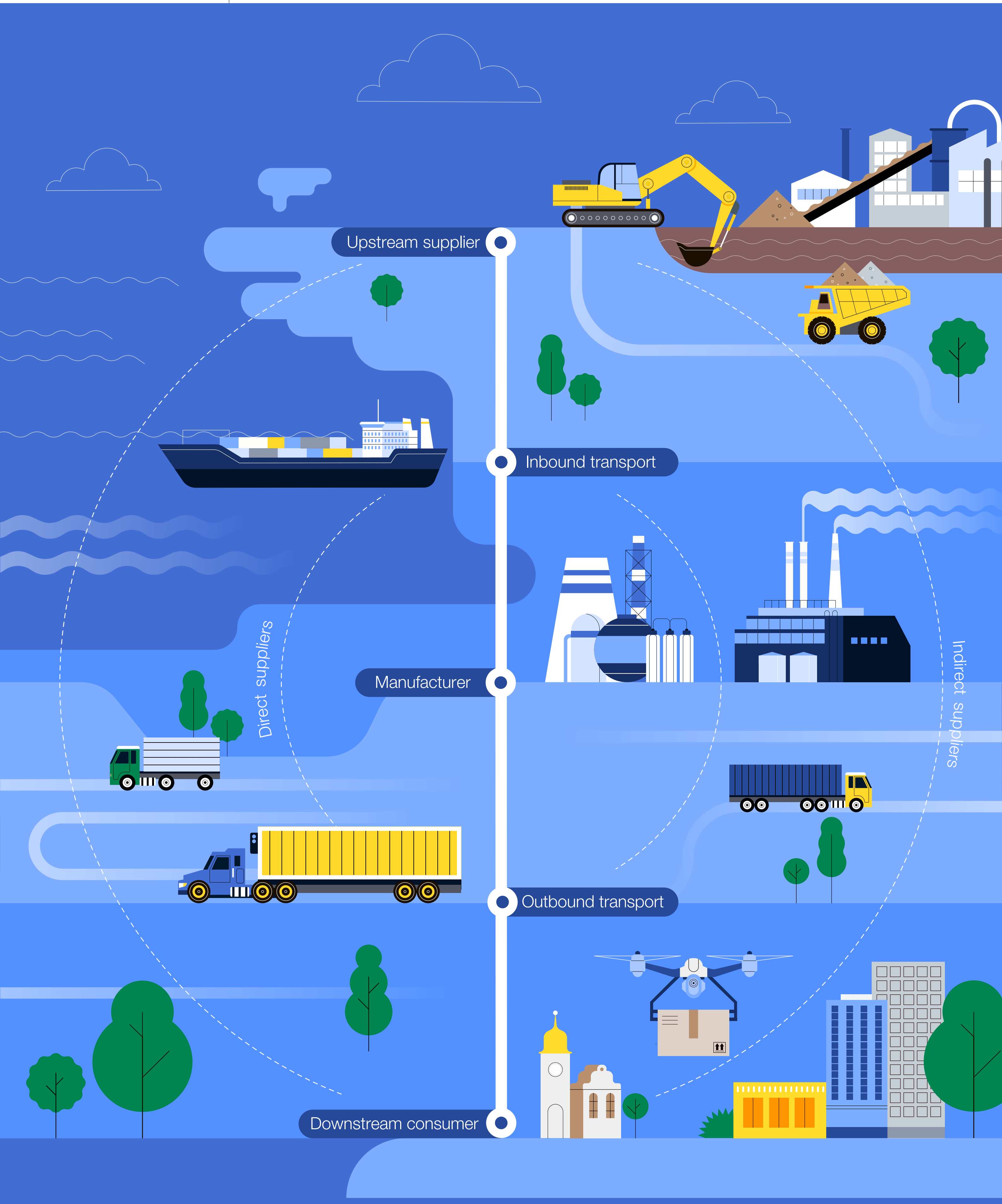
Over the past decade, digital transformation has accelerated within the sector, with continuous investments in innovation and emerging technologies such as digital twins, robotics, generative artificial intelligence (GenAI), cloud computing and the industrial internet of things (IIoT).[1] While this progressive digitalization fosters growth, efficiency and profitability, it also connects industrial and operational technologies (OT) to the digital world, exposing the sector to cyberthreats.

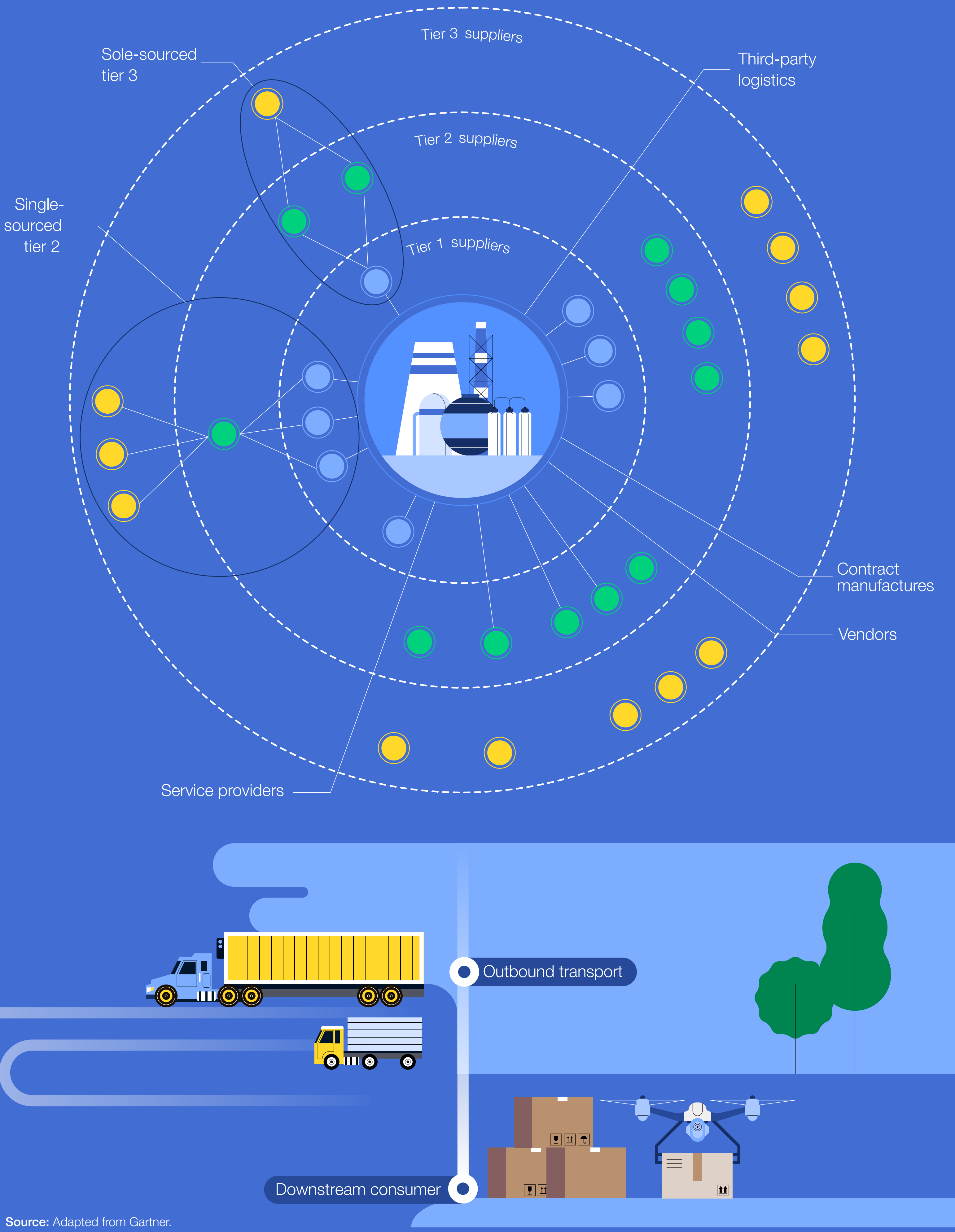
Heightened connectivity of the manufacturing digital ecosystem to various enterprise systems, the internet, cloud providers and service providers presents significant challenges in the industrial OT environments. This transition from traditional air-gapped systems to hyperconnected environments augments cybersecurity risks. Furthermore, discrepancies in investments between low- and high-revenue organizations exacerbate these challenges.[2] The boost in data exchange with the entire supply chain, including small and medium enterprises (SMEs) that are typically low-tech, has increased this risk.

The upsurge in connectivity and data transparency in the manufacturing ecosystem has expanded the sector's exposure, making it, for three years in a row, the sector most targeted by cyberattacks, accounting for 25.7%,[3] with ransomware comprising 71% of these attacks.[4] Given the complexity of modern supply chains, disruptions along the manufacturing process can have system-wide cascading effects, beyond the control of any single entity.

The inherent complexities of manufacturing and supply chains demand a holistic approach to mitigating cyber risks. Embedding a culture of cyber resilience in the organization's DNA is essential.

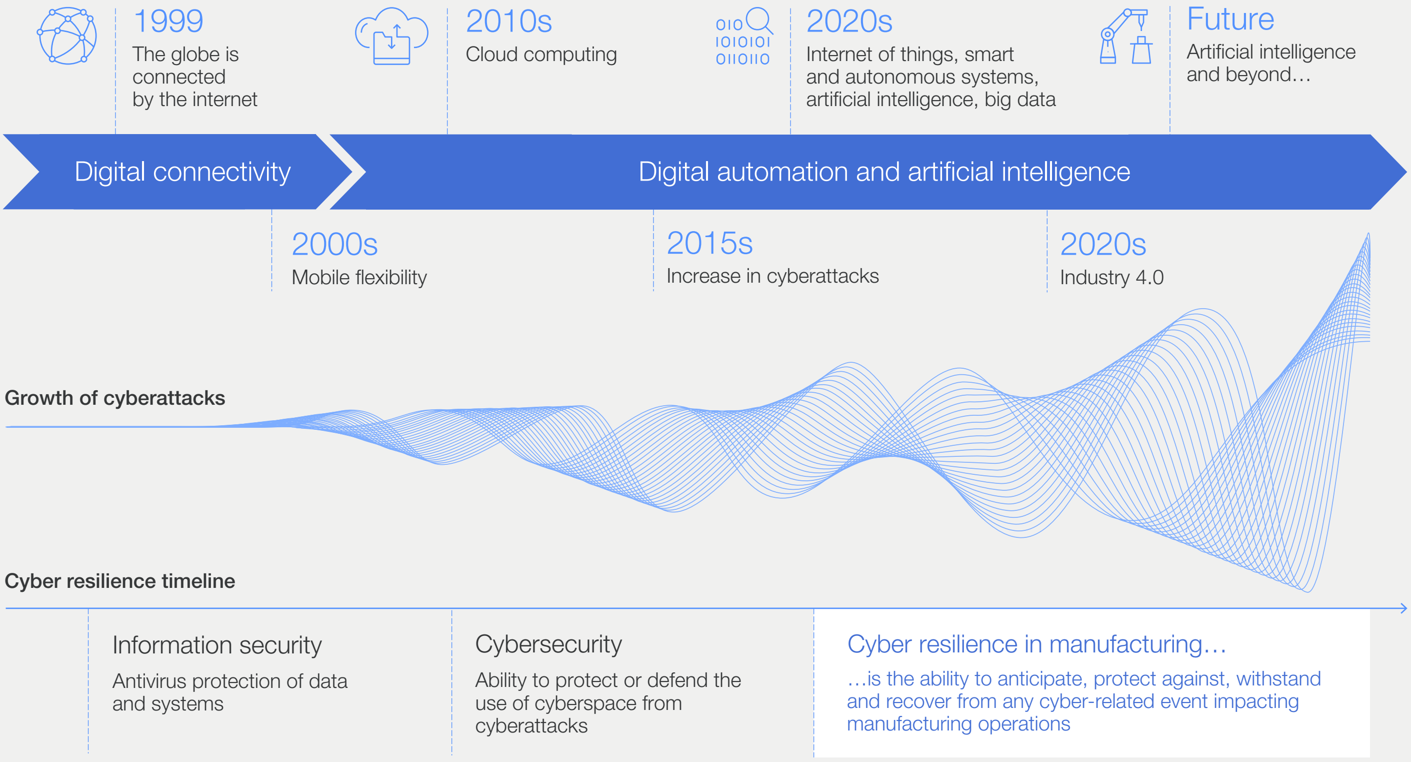
FIGURE 1 The manufacturing ecosystem





Source: Adapted from Gartner.

FIGURE 2 | Increasing cyberthreats in manufacturing require an evolution of cyber resilience



1999
The globe is connected by the internet

2010s
Cloud computing

2020s
Internet of things, smart and autonomous systems, artificial intelligence, big data

Future
Artificial intelligence and beyond…

Digital connectivity

Digital automation and artificial intelligence

2000s
Mobile flexibility

2015s
Increase in cyberattacks

2020s
Industry 4.0

Growth of cyberattacks

Cyber resilience timeline

Information security
Antivirus protection of data and systems

Cybersecurity
Ability to protect or defend the use of cyberspace from cyberattacks

Cyber resilience in manufacturing…
…is the ability to anticipate, protect against, withstand and recover from any cyber-related event impacting manufacturing operations

Source: Siemens and World Economic Forum

1.2 The main cyber risks in manufacturing

Cyberattacks can not only disrupt businesses and supply chains, offsetting the gains from digitalization, but also result in financial, productivity, reputational and even physical damage. In fact, nearly 57% of cyberattacks on OT in 2022 had real-world physical consequences, including production and loading disruptions, fires damaging equipment and accidents putting shop-floor workers at risk.[5]

The tally of cyberattacks continues to surge year after year, with extortion-based attacks remaining a prominent type.[6] In 2023, ransomware payments reached an unprecedented $1.1 billion.[7] Over the course of 2023 alone, the number of ransomware attacks on industrial infrastructure doubled, posing a significant threat to supply chain and manufacturing operations.

Ransomware remains the top-of-mind concern for manufacturers with 40% of the Cyber Resilience in Manufacturing survey respondents[8] ranking it first. According to recent research, ransomware attacks on industrial organizations increased by nearly 50% in 2023, with 71% of attacks directed at manufacturers.[9]

Manufacturing organizations present an attractive target for ransomware attacks, given their low tolerance for downtime and their relatively low level of cyber maturity compared to other sectors. Furthermore, these industries frequently underinvest in cyber resilience, primarily due to the substantial costs associated with redesigning manufacturing lines and upgrading equipment.[10]

Among the significant risks facing manufacturing organizations, social engineering and phishing, ranked as the second most prominent cyberthreats overall, were identified by 34% of survey respondents. Following closely, supply chain attacks secured the third position. Insider threats and denial of service attacks ranked lower in the overall hierarchy of cyberthreats for the survey respondents overall.

However, respondents from the health and healthcare sector ranked insider threat as their second most concerning cyberthreat, alongside ransomware, with supply chain attacks taking the top spot. Similarly, participants from the food and beverage industry also highlighted insider threats as a top concern, followed by social engineering and ransomware.

To reap the benefits of digitalization, it is crucial for the manufacturing sector to be prepared against the growing threat landscape and become cyber resilient.

FIGURE 3 | Top five cyber risks to manufacturing

1 → **Ransomware**

A type of attack where threat actors take control of a target's assets, encrypt them and demand a ransom in exchange for the return of the asset's availability. Attackers can breach intellectual property (IP) information, access victims' data and block critical systems belonging to manufacturers or their critical third parties, disrupting day-to-day business activities.

2 → **Social engineering attack**

Exploits people by benefiting from human error or behaviour to access information or services. It uses manipulation to trick victims into giving away sensitive information. Common methods include phishing, spear-phishing and other tactics like baiting and scareware.

3 → **Supply chain attack**

Focuses on the interactions and connections between organizations and their suppliers. Attackers use the service supplier's vulnerabilities to access or disrupt the manufacturing organization. Attack techniques include: malware infection, social engineering, brute-force attack, exploitation of software vulnerability or configuration vulnerability, physical attack and counterfeiting.

4 → **Insider threat attack**

Leverages an insider personnel's authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent or unintentional acts that negatively affect the integrity, confidentiality and availability of the organization, its data, personnel or facilities.

5 → **Denial of service (DoS) or distributed denial of service (DDoS)**

Accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, prevents access for legitimate users. This prevents legitimate users from accessing information systems, devices, insider personnel or other network resources.

Source: Cyber resilience in Manufacturing Survey; ENISA Threat Landscape 2023;[11] NIST[12]

1.3 The global impact of cyberattacks

With production facilities spanning the globe, each interconnected entity acts as both a producer and a consumer, creating a complex network vulnerable to cyberthreats. Consequently, a cyberattack on one company can trigger ripple effects across the entire ecosystem, leading to costly consequences.[13]

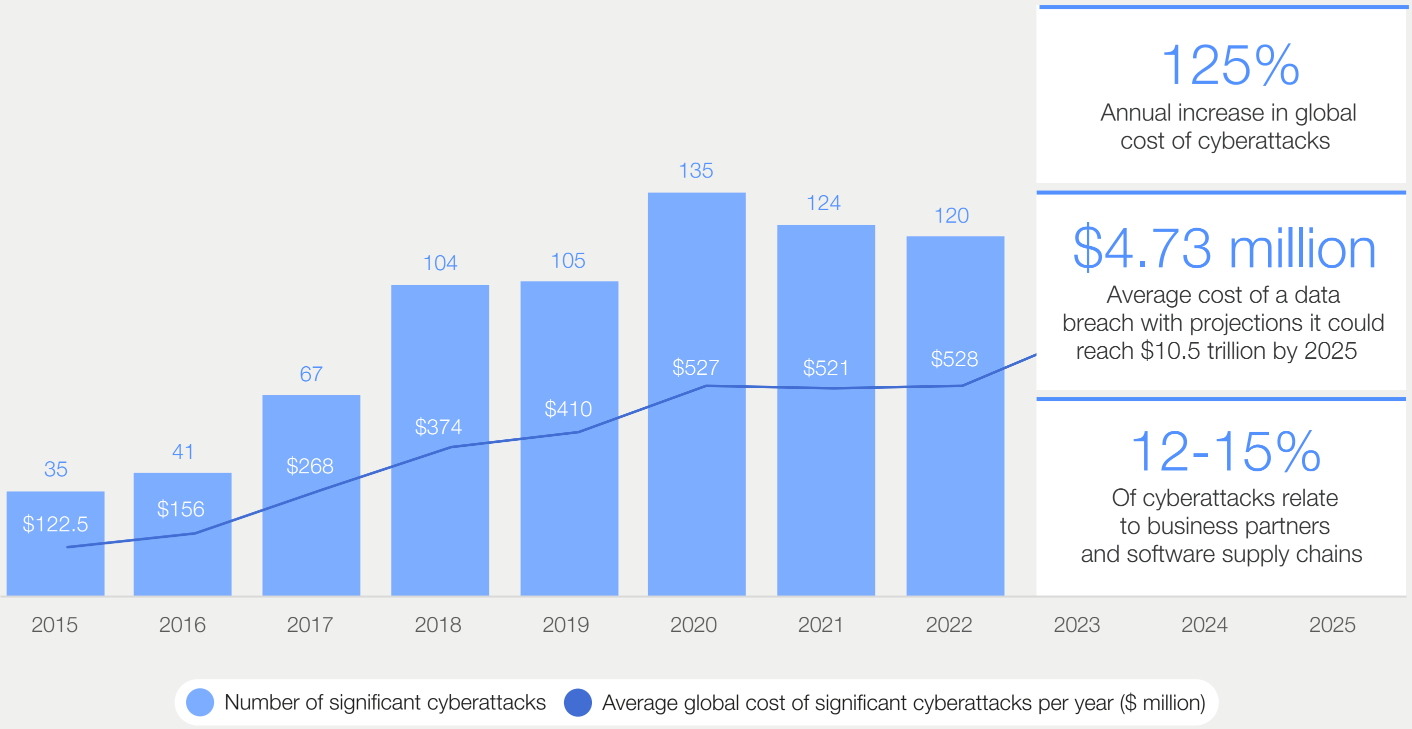
The resulting risks are systemic, contagious and often beyond the understanding or control of any single entity. According to the Global Cybersecurity Outlook 2024, 54% of organizations lack adequate visibility into the vulnerabilities of their supply chain. Additionally, 41% of organizations that suffered a material impact from a cyberattack reported that the breach originated from a third party.[14]

Recent cyber incidents further highlight the immense financial and operational toll of such attacks. For instance, in February 2024, a German battery manufacturer experienced a significant cyberattack, resulting in production halts at five plants for over two weeks.[15] In 2023, a ransomware attack on a large semiconductor industry supplier resulted in an estimated cost of $250 million in the next quarter.[16] Similarly, in 2022, a prominent car manufacturer was forced to suspend production at 14 plants for a day, leading to an estimated output loss of 13,000 cars, due to a cyberattack against a components supplier.[17]

The Cyber Resilience in Manufacturing survey (please see the Methodology) identifies business disruption as the primary impact of cyber incidents, with 60% of respondents highlighting its significance. These findings align with the Global Cybersecurity Outlook 2024, where 45% of leaders expressed operational disruption as their greatest concern in the event of a cyber incident. Safety concerns ranked second, with 35% of respondents, followed by potential damage to customer assets. These insights emphasize the profound and far-reaching impact of cyberattacks within the manufacturing sector and the urgent need for robust cybersecurity measures to safeguard its integrity.

FIGURE 4 **The impact of cyberattacks worldwide**

The cost of cybercrime has **increased 125% per year** on average, with the impact of a successful cyberattack reaching **$4.73 million** per attack in industrial settings. If this growth continues, the projected global impact could reach **$10.5 trillion by 2025**



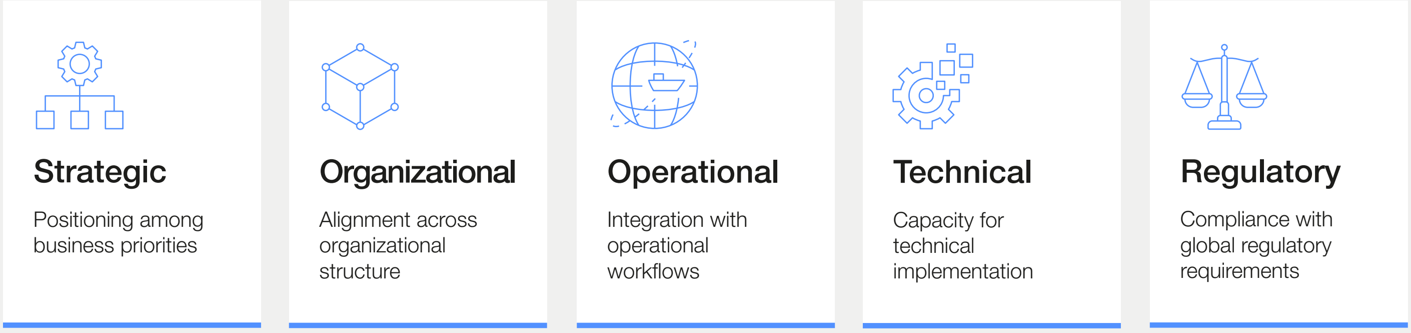
Source: McKinsey & CO, IBM 2023 Cost of a Data Breach Report, World Economic Forum analysis.

2 Towards a cyber resilient manufacturing sector: Uncovering the challenges

Organizational challenges rank as the top dimension inhibiting the adoption of a cyber resilient culture.

The manufacturing sector operates within a complex ecosystem characterized by diverse sites, extensive supply chains and interconnected networks, which rely on numerous suppliers, vendors and partners. While the sector reaps the benefits of digitalization and emerging technologies, it also grapples with challenges across five dimensions, each presenting unique hurdles on the path to cyber resilience.

FIGURE 5 Five key dimensions of challenges in manufacturing



Strategic
Positioning among business priorities

Organizational
Alignment across organizational structure

Operational
Integration with operational workflows

Technical
Capacity for technical implementation

Regulatory
Compliance with global regulatory requirements

2.1 Divergent cultures and resources

Divergent organizational culture between enterprise and industrial environments presents the most significant obstacle to cybersecurity efforts, according to the Cyber Resilience in Manufacturing survey (please refer to Methodology).

- **Distinct priorities.** IT and OT teams traditionally work at different ends of the technology stack and data flow. They tend to approach, prioritize and govern cybersecurity differently. Lack of collaboration on a formal IT/OT convergence strategy hinders secure digitalization of industrial environments.
- **Fragmented cybersecurity governance.** Many organizations lack a comprehensive cybersecurity governance framework, leading to decentralized decision-making at the manufacturing site level and hence increased risk. Effective cybersecurity governance requires awareness, training and incentives across all operational sites, making sure they all integrate cybersecurity into daily hygiene routines, similar to already existing practices for employee safety, product quality and equipment maintenance and integration.

- **Distribution of responsibilities.** With the increased pressure on business to cut cost and increase profitability, many organizations tend to have people wearing multiple hats and performing various tasks, ignoring the importance of segregation of duty and the associated risks. For example, database administrators may serve as system administrators, enabling them to have overarching rights to delete logs and cover up instances of fraud.

- **Talent shortage.** The global cybersecurity talent shortage, reaching nearly 4 million, is further exacerbated in the manufacturing sector, where the shortage surpasses 67%.[18] Finding and retaining talent with expertise in both cybersecurity and manufacturing operations can be difficult, making the cyber resilience journey harder.

2.2 Increased connectivity and legacy systems

Technical challenges have been recognized as the second largest hurdle to cyber resilience. The convergence of outdated legacy systems with the proliferation of connected assets within industrial control systems has engendered an environment inadequately prepared to withstand the sophisticated tactics and capabilities wielded by cybercriminals.

- **Legacy systems.** Legacy OT and industrial control systems introduce significant vulnerabilities due to outdated designs and limited access management. Despite their age, these systems remain integral to manufacturing operations, functioning as they were originally intended. However, the challenge lies in their inability to adapt to modern cybersecurity standards and to the evolving threat landscape. Compounding this issue is the reluctance to replace these systems due to the high costs involved, as well as their interconnected nature. Consequently, financial resources are often redirected to more immediate operational needs, leaving legacy systems vulnerable. With nearly 71% of these systems lacking proper support and robust access management procedures, the risks associated with legacy infrastructure are escalating rapidly, doubling year by year.[19]

- **Emerging technologies** present a double-edged sword, bringing both opportunities and challenges to cybersecurity. Investments in cutting-edge technologies introduce complexity and new risks, requiring a holistic and comprehensive update of cybersecurity strategies. For instance, the proliferation of highly connected industrial internet of things (IIoT) devices and the widespread adoption of artificial intelligence (AI) aim to improve service delivery and productivity. However, they also create new points of entry and expand the attack surface for malicious actors, requiring proactive adjustments of cyber education, risk assessment and validation protocols.

- **Software reliance.** Most manufacturing processes, operations and key applications are based on software applications. In fact, software plays a crucial role in optimizing processes, increasing efficiency and ensuring product quality for key areas such as procurement, invoicing and supply chain automation. These processes are crucial and their hyperconnectivity and interoperability complicates the task for manufacturers and their suppliers to ensure a good security posture.[20] While managing the large software environment and its connectivity is cumbersome, the fact that an average of 77%-90%[21] of any given piece of modern software is open-source software makes it even harder to control and attest for its security. The recent example of the XZ backdoor highlights this problem, given that the backdoor was introduced in 2021 and only discovered in 2024.[22]

2.3 Operational sensitivity to downtime and extended ecosystem dependencies

Operational challenges hinder manufacturing resilience, ranking third among the challenges in the survey, given the digitalization and automation of manufacturing operations and their often-continuous throughput requirement.

- **Downtime sensitivity.** Limited downtime tolerance makes manufacturing companies prime targets for ransomware attacks, constraining regular system updates and patches.

- **Ecosystem risks.** As manufacturing facilities embrace interconnected data-driven processes, reliance on cloud services and remote maintenance operations, the scope of risk extends beyond traditional supply chains to encompass a broader ecosystem. This intricate network of dependencies challenges cybersecurity strategies, requiring a comprehensive mapping to address both direct and indirect risks.

- **Pace of digitalization:** Rapid digitalization drives the need for new expertise in both internal (e.g. industrialization) and external (e.g. robotics and AI) domains to manage evolving risk profiles effectively.

2.4 Strategic alignment with business priorities

Strategic challenges arise from the dynamic tensions between economic factors, market forces and geopolitical tensions.

- **Integrating cybersecurity strategy into business priorities** remains a persistent challenge for most organizations, as they often prioritize short-term business objectives over investing in long-term resilience measures.

- **Continuously shifting market dynamics** further complicate strategic decision-making and hinder cybersecurity investments and prioritization, as organizations grapple with the need to adapt quickly to new market demands or competitive threats.

- **Increasing geopolitical tensions** impact manufacturing organizations both digitally and physically. Decentralized operations and reliance on global IT and OT suppliers amplify these challenges, requiring robust cyber resilience strategies.

2.5 Widespread and complex regulatory landscape

Manufacturing organizations must adhere to various regulations and industry standards related to human and product safety, data protection and cybersecurity. The decentralized operational environment and fragmented and diverse local, regional and industry-specific regulatory landscapes add another layer of complexity to cybersecurity efforts.

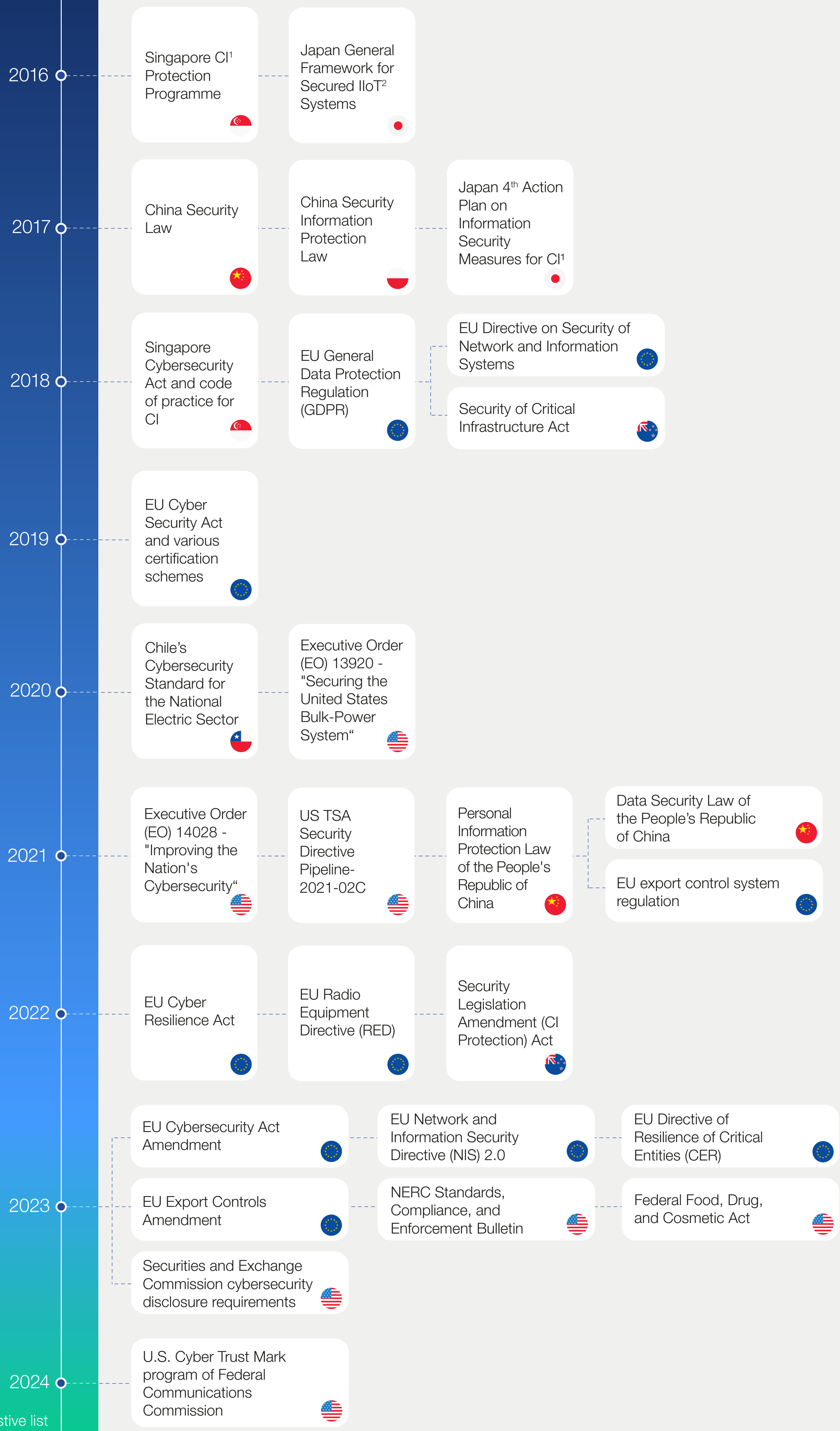
- **Widespread regulations** pose a significant challenge for the manufacturing sector. For example, in the European Union, a new legislative proposal, the Cyber Resilience Act, is being discussed to introduce mandatory cybersecurity requirements for hardware and software products throughout their life cycle. Additionally, legislations such as the updated Network and Information Security (NIS 2) and Critical Entities Resilience (CER) directives classify certain manufacturing industries as “essential entities,” mandating them to manage their security risks and prevent or minimize the impact of incidents on recipients of their services. Due to the large variety of requirements, organizations have to adapt their operations and products to local and regional requirements. At the same time, the different incident reporting requirements and timelines challenge organizations on their response mechanisms and reaction time.

- **Legislative developments:** In the United States (US), federal regulations target specific sectors like water, transportation and pipelines and a national cybersecurity strategy was released in March 2023. The US Cybersecurity & Infrastructure Security Agency’s Cross-Sector Cybersecurity Performance Goals outline cybersecurity practices that all critical infrastructure entities, large or small, should voluntarily implement to reduce risks to both critical infrastructure operations and US citizens.[23] The country's Securities and Exchange Commission has set a new precedent by charging a software company and its chief information security officer with fraud for internal control failures relating to allegedly known cybersecurity risks and vulnerabilities.[24]

- **Standards and Frameworks:** The International Society of Automation (ISA)/International Electrotechnical Commission's (IEC) ISA/IEC 62443 is considered by many to be the primary cybersecurity standard for industrial control systems. It currently includes nine standards, technical reports and technical specifications.[25] The US government's National Institute of Standards and Technology's (NIST) Cybersecurity Framework Version 1.1 Manufacturing Profile offers a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The new NIST Cybersecurity Framework 2.0 also provides a voluntary framework to help manufacturers safeguard their cybersecurity posture. In addition, cybersecurity has been identified as a key risk for business and has been introduced as an additional requirement for quarterly review at the board level as part of the environmental, social and governance (ESG) strategy.[26]

Additionally, the SANS Institute, a leading cybersecurity training and research centre, has published "The 5 Critical Controls for ICS/OT Cybersecurity", highlighting the most pressing controls based on an analysis of all the known cyberattacks on industrial control systems.[27] However, there is no overarching "cybersecurity gold standard" tailored specifically for manufacturers, one that would comprehensively address the different sectors' and countries' interdependencies and establish security requirements beyond the existing frameworks and IT standards.

FIGURE 6 | **In recent years there has been a rise in global cyber policies and regulations increasing the complexity for manufacturing**



2016
- Singapore CI[1] Protection Programme
- Japan General Framework for Secured IIoT[2] Systems

2017
- China Security Law
- China Security Information Protection Law
- Japan 4th Action Plan on Information Security Measures for CI[1]

2018
- Singapore Cybersecurity Act and code of practice for CI
- EU General Data Protection Regulation (GDPR)
- EU Directive on Security of Network and Information Systems
- Security of Critical Infrastructure Act

2019
- EU Cyber Security Act and various certification schemes

2020
- Chile's Cybersecurity Standard for the National Electric Sector
- Executive Order (EO) 13920 - "Securing the United States Bulk-Power System"

2021
- Executive Order (EO) 14028 - "Improving the Nation's Cybersecurity"
- US TSA Security Directive Pipeline-2021-02C
- Personal Information Protection Law of the People's Republic of China
- Data Security Law of the People's Republic of China
- EU export control system regulation

2022
- EU Cyber Resilience Act
- EU Radio Equipment Directive (RED)
- Security Legislation Amendment (CI Protection) Act

2023
- EU Cybersecurity Act Amendment
- EU Network and Information Security Directive (NIS) 2.0
- EU Directive of Resilience of Critical Entities (CER)
- EU Export Controls Amendment
- NERC Standards, Compliance, and Enforcement Bulletin
- Federal Food, Drug, and Cosmetic Act
- Securities and Exchange Commission cybersecurity disclosure requirements

2024
- U.S. Cyber Trust Mark program of Federal Communications Commission

Non-exhaustive list

1. CI: Critical infrastructure

2. IIoT: Industrial internet of things,
3. OT: Operational technology

Source: World Economic Forum; press releases; Schneider Electric, BCG and Accenture analysis

3 Guiding principles

Making cyber resilience a core part of the organizational DNA is essential to navigate cyber risks across the manufacturing sector.

The three guiding principles aim to support manufacturing and supply chain leaders in establishing a strategy to deliver an overarching cybersecurity culture across their organizations. These principles complement existing frameworks, standards and regulations.

The principles have been formulated after extensive research and consultations with industry leaders and standards and regulatory bodies as well as insights from the Cyber Resilience in Manufacturing initiative. Each principle is supplemented with additional guidance, key considerations and use-cases to facilitate adoption and effective implementation.

FIGURE 7 **Guiding principles to build a cyber resilience culture in manufacturing**

Make cyber resilience a business imperative

Embed cyber resilience into the organizational DNA, from leadership to shop floor.

- Lead from the top
- Establish cybersecurity governance
- Secure budget and resources
- Create incentives

Drive cyber resilience by design

Integrate cybersecurity into every process and asset to foster a cyber-resilient environment.

- Invest in education and training
- Include cybersecurity in critical business processes
- Continuously improve operational assets
- Prepare to respond to and recover from any cyber incident

Engage and manage the ecosystem

Engage with the ecosystem to build trusted partnerships, manage risks and raise security awareness

- Identify key stakeholders
- Establish cybersecurity baselines
- Ensure consistent oversight
- Keep learning

3.1 Make cyber resilience a business imperative

Making cyber resilience a core part of the organizational DNA is essential to navigate cyber risks across the manufacturing sector.

The key elements to make cyber resilience a business imperative revolve around cultural change; comprehensive cybersecurity governance; securing budget and resources; and creating incentives to ensure cybersecurity is an objective that all stakeholders relate to.

Lead from the top

Effective culture change always originates from the top, which is why it is imperative for manufacturing and supply chain leaders to personally champion the necessary mindset shift and serve as exemplary role models.

Key considerations:

- Ensure continuous education: Leaders must invest time in learning foundational cyber resilience strategies. It's crucial that they not only grasp the vital disruption created by cybersecurity risks but also stay current on the ever-evolving threat landscape.
- Lead by example: Embodying the principles of cyber resilience in their actions and communications, leaders can inspire their teams to adopt a proactive approach to cybersecurity. This, in turn, safeguards critical operations and assets against evolving threats.[28]
- Need for Cultural Change: leaders must recognize the imperative for a mindset shift across their organization. Traditional manufacturing and supply chain culture, typically centred around cost, cash, efficiency and service, may inadvertently overlook cybersecurity requirements, leaving vulnerabilities in an increasingly digital landscape.
- Advocacy for Cyber Resilience: leaders should vocally for cyber resilience. This entails seamlessly integrating it into the existing fabric of the supply chain culture, akin to the longstanding emphasis placed on people safety or product quality.

Key questions for manufacturing and supply-chain leaders

Are senior leaders actively championing the importance of cyber resilience?

How can leadership – at all levels – better integrate cyber resilience into the organizational culture?

Establish cybersecurity governance

Establishing robust governance is paramount to driving responsibility and accountability throughout the organization. This allows a clear definition of the ownership of the cybersecurity risks, but also defines how organizations structure their action plan from top leadership down.

Key considerations:

- Integrate cybersecurity for manufacturing into the organization's overall enterprise risk management strategy.[29] A comprehensive cybersecurity culture requires clear governance and strong leadership commitment to champion cyber resilience goals from the top down.[30] This involves establishing clear policies, pragmatic procedures, regular checks and ongoing monitoring to address deviations promptly.
- Set and clarify roles and responsibilities. Each employee should i) be aware of their role pertaining to cybersecurity; ii) understand their responsibilities; and iii) be held accountable. Making sure employees have well-defined roles and responsibilities ensures proper controls and reduces the risk of cyberthreats.
- Set collaboration models. Cybersecurity is not a single-person/single-team effort. It must extend to every part of the organization, including the plant floor. The chief information security officer (CISO)/security team needs to develop a productive relationship with manufacturing leaders and employees. The creation of an IT and OT security executive steering committee, comprising leadership from across IT and OT, ensures alignment at the top to drive sub-teams. Also, adding personnel from the OT infrastructure team to the enterprise security and security operations centre (SOC) teams creates more operations-related awareness in the security team.

Key questions for manufacturing and supply-chain leaders

Do we have clear roles and responsibilities defined for cybersecurity across the organization?

Are cybersecurity policies and procedures well-defined, visible and regularly reviewed?

Secure budget and resources

Securing adequate budget and resources for cybersecurity initiatives is paramount to fostering a resilient cyber environment. Given the traditional focus on capital and cost efficiency as well as operational effectiveness, leaders must strategically allocate resources to address cybersecurity needs effectively.

Key considerations:

- Secure cybersecurity foundations, such as budget allocation for dedicated cybersecurity leaders, upgrades of obsolete legacy systems, and conduct of awareness and training campaigns. By investing in these critical areas, organizations can establish a strong cybersecurity posture and mitigate potential risks.
- Ensure dedicated staffing and effective collaboration by dedicating cybersecurity staff, both centrally and in proximity to manufacturing and supply chain operations, to continuously improve cybersecurity capabilities. Collaborate with internal stakeholders such as IT and security teams, as well as external partners and vendors, to maximize the efficiency of cyber resilience investment strategies.
- Adopt strategic resource allocation and agility by prioritizing investments – whether related to staffing, solutions or infrastructure – based on risk assessments and organizational priorities.

Key questions for manufacturing and supply-chain leaders

Have we allocated sufficient budget and resources to support cybersecurity initiatives?

How can we ensure ongoing financial support for cybersecurity efforts?

Create incentives

Establishing incentives to prioritize cybersecurity as an objective that all stakeholders in manufacturing environments relate to is of fundamental importance.

Key considerations:

- Advocate for compelling cyber career paths that not only encompass vertical cybersecurity roles but also facilitate cross-pollination with manufacturing and supply chain career paths. Encourage professionals from various profiles in the OT environment to explore rewarding opportunities in cybersecurity.

- Establish a recognition and reward framework. Recognize and empower cybersecurity champions across all organization levels. Incorporate cybersecurity as a key performance indicator (KPI) and reward employees accordingly. Align reward systems to encourage adherence to cybersecurity protocols and proactive threat identification.

- Create healthy competition. Benchmark peers while creating an information-sharing culture based on rewards. Adjust the reward systems to incentivize adherence to cybersecurity protocols, from proactive threat identification to systematic incident reporting and response.

- Cultivate a culture of transparency, where issues are swiftly elevated, embracing the mantra that “bad news should travel fast”. Ensure that mistakes are not stigmatized and issues are investigated with rigour, seeking to understand and learn.

Key questions for manufacturing and supply-chain leaders

Are incentives in place to encourage proactive cyber resilience behaviours among employees?

How can we improve our reward systems to promote both compliance and ongoing learning?

CASE STUDY 1

Unilever
Leveraging factory cybersecurity champions

In response to the evolving landscape of cyberthreats, Unilever embarked on a transformative programme to fortify its cyber defences across its factories worldwide. Central to this initiative was the establishment of a robust “Factory Cyber Security” organization. At its helm stands a “Global Factory Cyber Security Leader”, orchestrating a cohesive programme to protect Unilever’s manufacturing operations – made up of “work packages” that cover four deliverables: identify, protect, detect and response.

Complementing this global leadership are eight “Regional Cyber Security Champions” stationed strategically across the globe. These champions serve as linchpins between the global strategy and local execution, fostering a network of resilience spanning over 200 factories. Collaborating closely with these regional champions are local “Factory Cyber Security Champions”, embedded within each facility, ensuring tailored and responsive protection at the grassroots level. For the sake of transparency, the global and regional roles are funded by cyber security, while the local factory roles are funded by each individual factory.

Integral to this framework is the continuous education and training provided by the global and regional champions. Armed with cutting-edge cyber tooling knowledge and a keen eye for identifying and mitigating risks, they empower local champions to proactively defend against emerging threats, thereby fortifying Unilever’s cyber defence posture at every level of operation.

CASE STUDY 2

Volkswagen Group

Establishing industrial cybersecurity governance from leadership to shop floor

Industrial cyber security takes care of securing the production process with the equipment and systems used against cyberthreats. Specifications, processes, practices and technologies are used to detect, defend against and deal with cyberattacks and other unwanted activities. This includes the protection of components, networks and data as well as the establishment and compliance with processes and organizational requirements.

A "group regulation" implemented in 2022 demonstrates Volkswagen's cybersecurity governance mandate at the corporate level. All brands and locations of the Volkswagen Group are supported by an "Industrial Cyber Security Group Information Security Team" by defining and maintaining information security requirements on the shop floor. The team, consisting of nine people, is giving support by providing advice, ensuring transparency about risks in the group, developing blueprints and solutions for the shop floor and promoting the transfer of knowledge between all stakeholders on information security issues in production.

By conducting cybersecurity assessments in various plants all over the world, the maturity level is evaluated, to be continuously improved and reported to the top management in the information technology and production department. The "Production Information Security Officer", as the person responsible for cybersecurity in each plant, is a key interface to the cybersecurity team. This role is constantly evolving through learning paths and mandates with competencies and responsibilities.

CASE STUDY 3

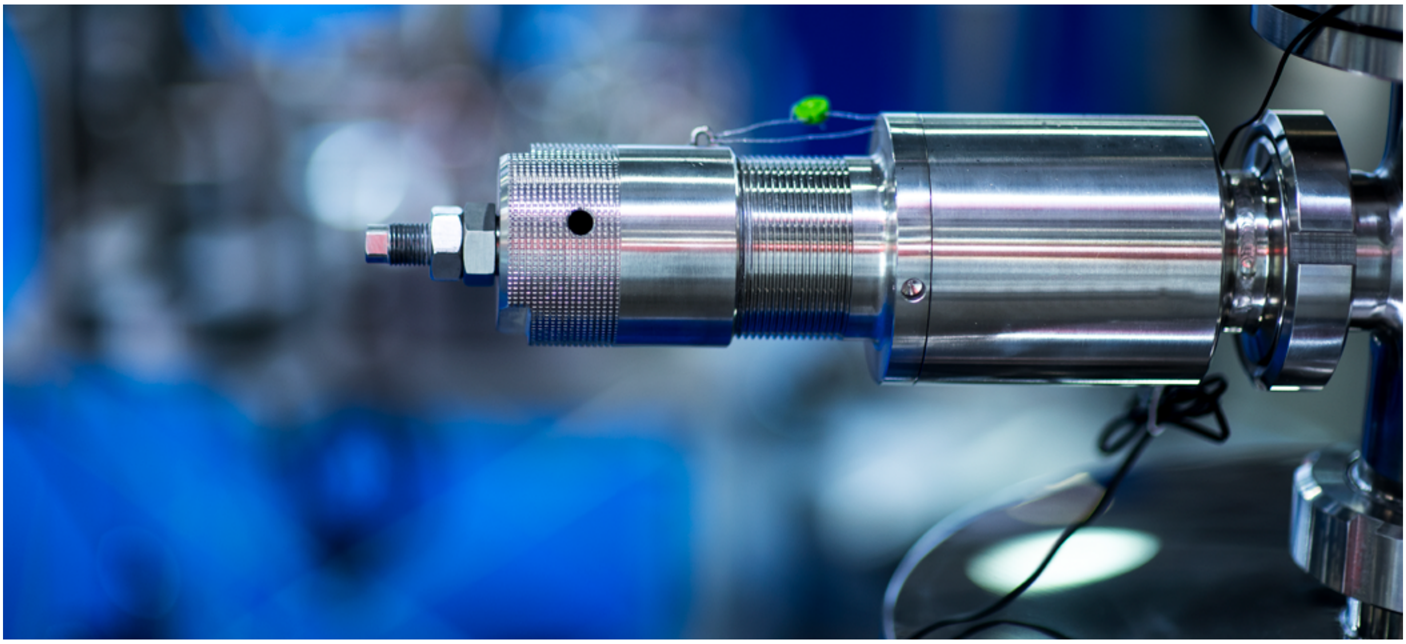
Henkel

Making manufacturing cyber resilience a priority by showcasing cyber risks

Henkel has more than 150 manufacturing sites globally across two business divisions. To improve OT security, it was important to make this a joint priority between supply chain organizations and the cybersecurity team. The cybersecurity risks had to be put into a business context, as well as in the light of staff safety, supply continuity and product quality.

In addition to general awareness measures, tangible, eye-opening interventions were identified to drive home the significance of OT security: an internal red team[31] conducted an actual compromise of a manufacturing site, compromising programmable logic controllers (PLCs), human-machine interfaces (HMIs), etc. – and capturing it on video.

This exercise made the risks tangible not only for personnel at the manufacturing site but through the video, to counterparts at other sites too. It demonstrated the resulting impact clearly and transparently, not only in abstract risk or cyber terms but tangibly from a supply-chain perspective.



CASE STUDY 4

Schneider Electric

Raising cybersecurity awareness for an inclusive cybersecurity culture

Schneider Electric integrates cybersecurity risk management into its manufacturing digitalization agenda. Committed to implementing cybersecurity controls on all industrial sites, the company has set itself the ambition of making all new manufacturing lines compliant with the IEC 62443 Security Level 2 (SL2). This ambition is set by the supply chain executive team, the effort is monitored and governed, and incentives are put in place to drive the right leadership and employee behaviour to achieve this goal. The elements of this systematic approach include:

- Executive support and joint governance from the global cybersecurity and supply chain functions: The cybersecurity objectives are defined by the global CISO and the implementation strategy for those requirements is carried out by global supply chain executives. Having the global CISO and supply chain executives co-lead this effort ensures that the effort is "led from the top" and places cyber security as a business imperative. Together, they secure and prioritize resources for a robust cyber posture and to drive the compliance with IEC 62332 SL2 for new manufacturing lines.

- Employee incentives: Employees play a critical role in achieving cybersecurity ambitions, since human errors are often the weakest link. It is important for leadership to encourage the right behaviour among all employees, including those on the manufacturing floor, for whom cybersecurity is not a core responsibility. The executive management team has added cybersecurity targets into the annual performance review of manufacturing employees. Adherence to the defined cybersecurity objectives is therefore tied to the performance of industrial sites in the internal performance management system called the "Schneider Performance System".

CASE STUDY 5

Johnson & Johnson

Cybersecurity culture as a fundamental imperative from shop floor to leadership

With the digitization of supply chain operations and interconnectivity of IT and OT, Johnson & Johnson realized the need to strengthen cyber resilience in manufacturing by establishing a strong cybersecurity culture.

As a large healthcare company with multiple sites globally, Johnson & Johnson has on-the-ground cybersecurity advocates to educate everyone at the site and coordinate site-level actions and responses. Inconsistent or reactive responsibility for security awareness and actions across more than 60 sites is a challenge for the security programme.

The following are some of the key actions the company took:

- Created a core team of IT and business leadership to lead the effort and define the roles and responsibilities of a "cybersecurity champion".

- Partnered with industry experts to build a plan with change management, training material, website, videos and an OT cybersecurity lab to incubate solutions.

- Connected with "make" and "deliver" leadership to nominate points of contact for each site to establish a network of cybersecurity champions.

- Successfully mobilized the cybersecurity champions network at each site.

The cybersecurity champion role has been instrumental as the liaison between site, business teams and cybersecurity. The champions collaborate with the cybersecurity team for risk assessments, remediation actions and any urgent needs to strengthen cybersecurity and resiliency.

3.2 Drive cyber resilience by design

Companies must integrate cyber resilience into every process and system using a risk-based approach to foster a cyber-resilient environment.

Cyber resilience should be integrated "by design" into every process and system. This means treating cyber resilience as a fundamental requirement in the development of new products, processes, systems and technologies.

Invest in education and training

Training should be continuous and ubiquitous.

Key considerations:

- Cultivate a learning culture. Embed cyber resilience in day-to-day behaviour and run year-long cybersecurity campaigns – every employee across every role should be cyber-aware. Provide insights and best practices on how leading companies are managing IT and OT convergence.

- Tailor education and training. Provide tailored training according to employee groups. Training should be continuous throughout the year and interactive. Leverage emerging technologies to improve the cybersecurity training experience, for example, with immersive experiences. Include and train service providers as part of safety training by providing acceptable user policies when they access or visit critical spaces.

- Foster cyber talent development and empowerment. Nurture cyber talent pools, and empower employees with clear accountability and skills to stay updated on emerging threats and mitigation strategies to safeguard the organization against cyberthreats.

Key questions for manufacturing and supply-chain leaders

Are employees at all levels – from the shop floor to the executive level – receiving adequate cyber resilience training?

How can we enhance cyber resilience education and training programmes to stay ahead of threats?

Include cybersecurity in business processes

Don't reinvent the wheel: integrate cybersecurity into the existing business processes to maximize efficiency.

Key considerations:

- Align and standardize company-wide cybersecurity processes by being mindful of OT and engineering differences.
- Embed cyber resilience into digital project and product design. Ensure that cybersecurity standards and requirements are part of each digital project and process from the inception phase. This should not be limited to digital products, but all the associated processes such as procurement, legal, and merger and acquisitions. Embed security needs by design, rather than bolting them on, as a key part of every digital project and product.
- Learn and reapply from existing quality and safety processes. Both quality and safety must be well-embedded into the manufacturing culture, both by internal employees and external vendors. For example, vendors should receive safety training before entering a plant. They should also be formally informed of the cybersecurity requirements at the plant.

Key questions for manufacturing and supply-chain leaders

Are employees at all levels receiving adequate cybersecurity training?

How can we enhance cybersecurity education and training programmes?

Continuously improve operational assets

Identify critical processes and design security around business objectives and outcomes.

Key considerations:

- Make asset management a priority. Maintaining an up-to-date asset inventory is the foundation for an effective cybersecurity programme. Such inventory helps tracking and managing all hardware and software assets within plants, including critical information assets such as network diagrams and device configurations.
- Adopt a risk-based architecture reference. Implement a defensible architecture for the manufacturing environment, including network segmentation, secure remote access and controls on the network, both directly on endpoints and within cloud environments.
- Ensure visibility and monitoring so that threats in the environment are detected quickly and response activities initiated. Ensure risk-based vulnerability management, patching and upgrades.

Key questions for manufacturing and supply-chain leaders

Have we integrated cybersecurity into our critical business processes effectively?

What measures can we take to ensure cybersecurity is a fundamental consideration in every process?

Prepare to respond to and recover from any cyber incident

Prepare the organization to confront any cyber incident through the development of risk-based incident management, response strategy, remediation and recovery plans.

Key considerations:

- Establish processes for incident management. Develop a risk-based approach and incident playbook(s) that include how to handle incidents in the company's factories as well as in suppliers, partners and service providers. Organizations should have an industrial control systems-specific incident response plan to respond to incidents in operational environments.[32] Establish minimum viable service levels for critical services to customers and partners and design systems to continue delivering through a crisis.
- Develop scenario planning. Understand the threat landscape and identify potential threats (including threat events, threat actors, etc.) that could target the IT and OT environments and their potential impacts.[33] Share information with the leadership and across the internal organization on the cyberthreats and risk-mitigation strategies. Conduct tabletop, red and blue team exercises, to test worst-case scenarios. If the skillset for managing a cybersecurity incident isn't available in-house, consider proactively establishing a relationship with an external incident response partner.
- Prepare plans and checklists. Have a remediation plan to support the timely restoration of normal operations to reduce the effects of cybersecurity incidents.[34] Develop a checklist of key ecosystem stakeholders, both internal and external. It should include key personnel, critical partners and law enforcement contacts, as well as vendors, OEMs, legal counsel, public relations contacts, government/regulators and customers that require notification, along with reporting timelines.

Key questions for manufacturing and supply-chain leaders

Do we have a robust incident response plan in place?

Have we conducted drills or simulations to test our readiness to respond to cyber incidents?

CASE STUDY 6

Unilever
Deploying a comprehensive OT cybersecurity strategy

A "Factory Cyber Security Programme" launched in 2019 encompasses a comprehensive approach to cyber securing operational technology (OT) assets. After engaging factory teams to carefully identify and catalogue all connected OT systems and associated high-level cyber issues, robust network segmentation was implemented, leveraging next-generation firewalls, to isolate OT assets from corporate IT infrastructure, ensuring a heightened security posture.

To enhance threat detection and response capabilities, endpoint detection and response (EDR) solutions were deployed across all factory environments. This allows for rapid identification and mitigation of potential cyberthreats, bolstering overall resilience. Concurrently, a proactive programme of patching and upgrading OT technology was instituted to eliminate exploitable vulnerabilities, further fortifying defences.

To provide ongoing visibility and oversight, each factory now benefits from a dedicated dashboard displaying vulnerability scores and performance metrics. This holistic approach not only ensures the integrity and security of OT assets but also underscores the company's commitment to proactive cyber defence within its manufacturing ecosystem.

CASE STUDY 7

Kuwaiti Danish Dairy (KDD)

Implementing controlled OT network access to enhance operational reliability

Establishing controlled network access to KDD's OT environments is crucial for protecting critical infrastructure while ensuring operational continuity and safety. The key challenges that the company has identified include dependency on IT network for user authentication, network broadcast storms and single points of failure.

To address these, network segmentation and access security controls have been implemented, including introduction of a dedicated domain controller for OT network authentication, controlled network segments between IT and OT networks, and site redundancy through storage virtualization.

These measures have minimized downtime, increased system availability for operations and allowed OT users to work seamlessly within the OT network. Broadcast storms have been reduced, leading to fewer disruptions and increased productivity. Failure at one data centre does not affect operations due to seamless operation from alternative data centres.

Proactive measures and collaboration have strengthened KDD's OT systems, prioritizing cyber resilience and improving system availability. Tailored cyber resilience strategies have protected critical infrastructure and enhanced operational reliability.

CASE STUDY 8

Siemens

Integrating cyber resilience into product design

With industrial digitalization and the increasing interaction between the IT and OT environments, Siemens saw its products and solutions open to new attack vectors in operational environments, particularly due to a lack of security controls. As a foundation for establishing security controls (authentication, signing, encryption, etc.) in operational environments, Siemens needed an infrastructure to securely issue certificates to its production facilities and the products being manufactured.

Siemens addressed the need to securely issue certificates to manufactured products with a "product PKI" (public key infrastructure). The Siemens Product PKI provides and manages certificates that are stored on and used by Siemens products and solutions. The certificates might be used in bootstrapping or other operational scenarios for authentication purposes. Or the certificates might be used to prove that a device is a genuine Siemens device.

Siemens integrated cybersecurity in product design and manufacturing engineering to foster a cyber resilient environment in its own facilities as well as in the industrial facilities of its customers.

CASE STUDY 9

Rockwell Automation

Achieving OT security certification for manufacturing facilities

With a mission to secure the connected enterprise for its customers and its own operations, Rockwell took steps to reduce OT technical debt, address outdated technology, remediated high-risk assets and solidified security controls across its manufacturing ecosystems. Rockwell's ultimate goal was to become a world-class leader in OT cybersecurity by meeting the very extensive 62443-3-3 set of industrial automation and control systems (IACS) security requirements, following the 62443-2-1 processes and controls. Rockwell's next goal was to help customers achieve the same results for their own plant operations.

Rockwell created a dedicated enterprise OT cybersecurity team focused on securing Rockwell's manufacturing facilities. After an extensive site analysis, a structured cyber framework was outlined that could continually mature the company's security posture by following industry standards including IEC 62443. The team achieved the certification goal using their own products, services and partner network and demonstrated to customers that they can help them on their own journey.

The creation of Rockwell's dedicated team and security framework has resulted in a manufacturing programme that instils a continuous improvement culture for maturing cyber security in OT environments resulting in manufacturing that's resilient, scalable, maintainable, secure and certifiable.

CASE STUDY 10

Schneider Electric

Integrating cyber resilience processes

Schneider Electric's cybersecurity strategy is multifaceted, covering the cybersecurity posture from IT to OT and from product design through installed base security. This strategy includes robust training and education of all its employees, both connected to and on the shop floor. This company-wide, end-to-end, risk-informed approach has significant preventative measures (breach readiness) while being able to respond and recover in case of an incident (breach resilience). Schneider Electric achieves these programmatic objectives with:

– Employee training and awareness: The company aims to raise employee cybersecurity awareness, provide relevant training and create a culture to empower employees across both IT and OT to act in a secure manner. The training includes an annual baseline awareness course for all employees and role-based trainings for specialized populations including shop-floor personnel. All training is created with people at the centre and used to support a culture of shared ownership of the cybersecurity posture by all employees.

– An enterprise risk management (ERM) framework: Using a company-wide cyber risk register to categorize risk, the company translates cybersecurity risks into business and operational scenarios and exposure. This exposure is communicated with the C-suite to drive investments in risk-mitigation initiatives. This framework is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and increases the company's overall level of cyber resilience.

– Secure development lifecycle (SDL) management: The SDL journey began over 10 years ago and its mature programme encompasses defined and implemented security requirements, product testing, vulnerability management capabilities and a formal cybersecurity review before release(s). The company's SDL programme is aligned to IEC 62443-4-1 and externally certified.

– Incident response capabilities: Schneider Electric is constantly testing and improving its capacity to respond to operational disruption, damage to customers, compliance issues and theft of intellectual property. Its incident response plans are defined and stress-tested routinely to ensure preparedness. A "Security Operations Center" operates 24x7x365 and is staffed with security analysts leveraging security incident and event management (SIEM) capabilities with OT scenario-based playbooks and responders.

The combination of these programmes ensures that cybersecurity risk is not an afterthought but part of the manufacturing management system.

CASE STUDY 11

Flex

Bolstering operational cyber resilience

Meeting the needs of a diverse set of customers can present challenges when balancing cybersecurity measures and demand for zero operational downtime.

Flex, a global, diversified manufacturer, tackled this challenge by developing and introducing a comprehensive technical programme, encompassing redesign of engineering equipment and policies, processes and procedures for cybersecurity mitigation and threat response.

Piloted at 25 manufacturing facilities, the new programme addresses critical aspects such as micro-segmentation, asset and threat visibility, and response and recovery protocols to help reduce the risk of downtime caused by cyber-attacks.

Engineers with expertise in non-cybersecurity domains joined the cybersecurity team, fostering closer collaboration with the operations and design teams. Additionally, Flex's engagement with OT vendors has helped enhance recovery capabilities, facilitate asset identification and deploy robust threat-monitoring mechanisms.

Through this programme, Flex continues to align cybersecurity awareness and safety with the specific needs of engineering teams, helping to mitigate risks and bolster operational resilience. This collaborative approach enables rapid, swift threat detection and response, reducing manufacturing and design operation interruptions and enhancing engineering asset security.

CASE STUDY 12

Engro Corporation

Securing OT-IT convergence against cyberthreats

In pursuit of excellence in its digital transformation, Engro faced the challenge of securing its OT-IT convergence where the potential interconnection of isolated plant systems with the outside world poses vulnerability to cyberattacks capable of disrupting production.

Engro institutionalized cyber governance by adopting global frameworks such as IEC62443, ISO27001 and NIST; conducted comprehensive consultant-led risk assessments of infrastructure; developed a three-tier strategy to improve cyber resilience; and cascaded these in the enterprise risk register for board-level visibility. Further, it reinforced the "Human Firewall" concept into the organizational culture by frequent cyber awareness campaigns and phishing simulations, and partnered with ISA (International Society for Automation) for human skill development.

Active engagement from the shop floor to top management led to the development of comprehensive OT security policies to integrate cyber resilience in the organization's DNA, promising "security-by-design" in the production life cycle. Ongoing integration of its IT and OT security operation centres will further enhance threat detection, investigation and incident response.

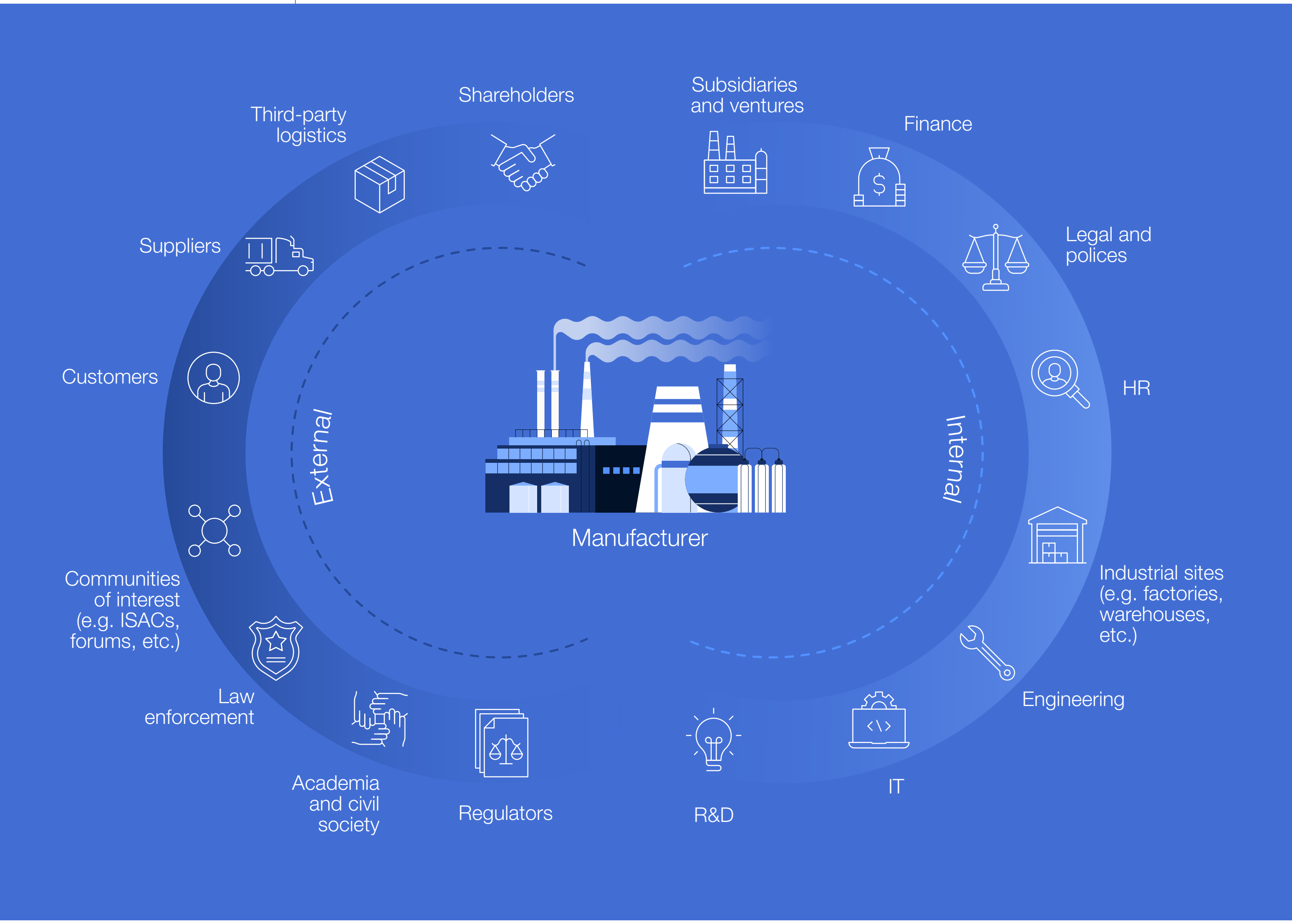
By implementing these measures, Engro has embarked on the journey of creating a secure digital environment for its people, process and products to boost the confidence of stakeholders to launch and further transform their business services while maintaining cyber resilience.

3.3 Engage and manage the ecosystem

Manufacturing organizations need to shift from supply-chain to ecosystem security to manage the systemic and cascading risks.

The manufacturing ecosystem is composed of a variety of stakeholders including raw material and packaging suppliers, production facilities, assembly lines, service providers, original equipment manufacturers (OEMs), vendors, logistics and transportation suppliers, information sharing and analysis centres (ISACs) and regulatory authorities. In the ecosystem, manufacturers are both suppliers and providers of products and/or components. Manufacturing organizations need to establish trusted partnerships by raising security awareness and security posture across the ecosystem.

FIGURE 8 **Engaging ecosystem stakeholders holistically**



Third-party logistics
Shareholders
Subsidiaries and ventures
Finance
Suppliers
Legal and polices
Customers
HR
External
Internal
Manufacturer
Communities of interest (e.g. ISACs, forums, etc.)
Industrial sites (e.g. factories, warehouses, etc.)
Law enforcement
Engineering
Academia and civil society
Regulators
R&D
IT

Identify key stakeholders

Identifying critical ecosystem members, pinpointing dependencies and assessing systemic risks from shared suppliers is essential.

Key considerations:

- Include the critical members of the ecosystem in cybersecurity risk assessments, and identify dependencies and systemic risks from common suppliers and vendors. Take advantage of threat information-sharing via ISAC communities.

- Prioritize suppliers by identifying the most critical and most vulnerable. This entails recognizing vendors that present a cybersecurity threat to manufacturing operations, as well as identifying critical suppliers whose operations could jeopardize production in the event of a cyberattack.

Key questions for manufacturing and supply-chain leaders

Have we identified all stakeholders within our ecosystem?

Do we understand the dependencies and interconnections among these stakeholders?

Align on cybersecurity baselines

Defining risk-based security profiles and integrating cybersecurity baselines for suppliers is a crucial step to ensure a comprehensive cyber resilience across the ecosystem.

Key considerations:

- Tier suppliers. Define risk-based security profiles and requirements based on the criticality of suppliers and vendors. Ensure executive support for ecosystem risk-management activities.

- Integrate cybersecurity baselines. Establish processes to limit financial and reputational damage by embedding cybersecurity controls in third-party contracts, and make cybersecurity standards and best practices contractually enforceable on partners and vendors.[35]

- Build trusted partnerships and ensure continuous dialogues with suppliers across the ecosystem. With the increased reliance on third-party products and software, collaboration ahead of integration and operation of products helps raise security awareness, alignment and security baselines.

Key questions for manufacturing and supply-chain leaders

Have we defined minimum cybersecurity standards for our ecosystem partners?

How can we ensure that these standards are consistently enforced?

Ensure consistent oversight

Organizations must ensure consistent monitoring of ecosystem vulnerabilities, conduct periodic reviews of processes and consistently apply regular patches and updates.

Key considerations:

- Ensure audit compliance. Enforce controls for vendor access to manufacturing, including secure remote access and policies for how vendors and service providers access manufacturing network and transfer files.

- Monitor the ecosystem regularly. With the rapid evolution of cyberthreats, it is important to monitor vulnerabilities internally and externally.

  While existing and globally recognized industry and cybersecurity certifications are great gatekeepers for the initial and yearly due diligence, it is key to keep open a continuous communication and review channel with critical stakeholders.

- Review and update. Ensure regular patching is aligned with the partner organizations in the supply chain. Continuously review processes and updates and implement a change management process.

Key questions for manufacturing and supply-chain leaders

Are we regularly monitoring and assessing cybersecurity risks within our ecosystem?

How can we improve our oversight mechanisms to better detect and respond to emerging threats?

Keep learning

Continuous learning is paramount for staying ahead of evolving cyberthreats and leveraging a cyber resilience culture.

Key considerations:

- Cultivate a robust learning culture, where the exploration of emerging threats and the analysis of past mistakes are not only encouraged but embraced. Foster an environment where openness and transparency are valued so that organizations can proactively address vulnerabilities and strengthen their cyber resilience capabilities.

- Establish an ecosystem-wide culture. Promoting collaboration and knowledge-sharing among cyber talents from various functions – for instance between IT and OT experts – enables individuals to glean insights from diverse perspectives and experiences, enriching their understanding of cybersecurity challenges and solutions.

Key questions for manufacturing and supply-chain leaders

Are we fostering a culture of continuous learning and knowledge-sharing around cybersecurity?

What steps can we take to empower employees to stay updated on the latest cyberthreats and mitigation strategies?

CASE STUDY 13

Schneider Electric

Partnering with the ecosystem to build a more resilient security posture

An ecosystem of stakeholder includes customers, suppliers, cross-industry organizations, authorities and national agencies. While all stakeholders are important and intertwined, recently, a focus on collaborating in the areas of supply chain and installed base security represented a unique and impactful output for Schneider Electric.

The company's supply-chain security programme addresses risks stemming from third-party suppliers, by building a holistic approach to value-chain security by implementing security controls at every level (R&D, design, manufacturing, distribution, staging, commissioning and operations). To achieve this objective, Schneider Electric takes both internal and external measures through policies and guidelines as well as external checks with audit and scoring agencies. Going beyond the internal posture by discussing with customers and authorities, it initiates shared responsibility and strives to adopt a common cyber posture.

Schneider Electric launched its installed base security initiative in order to reduce OT exposure risks in the customer's environment by chasing down outstanding vulnerabilities. The resulting OT threat intelligence capability provides its customers with visibility to enriched, contextualized and actionable exposure information to better secure their installations. This effort helps to foster trust with stakeholders within the ecosystem, sharing information in a manner that improves security along the value chain.

CASE STUDY 14

Siemens

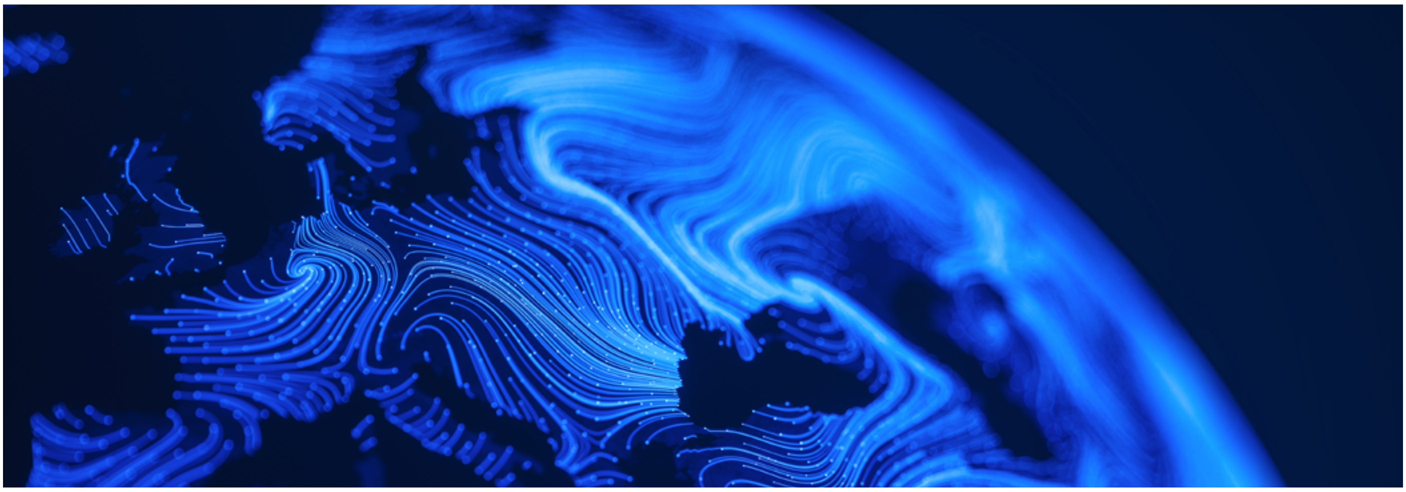
Establishing a supply-chain partner ecosystem

Around 2020, Siemens recognized the escalating threat of cybersecurity attacks on corporate supply chains and observed a rising frequency, severity and sophistication of attacks in its supply chain. It was obvious that no single player would be able to establish broader supply-chain security standards. On the contrary, collaboration and partnering were necessary.

Siemens embarked on a proactive journey to fortify its global cybersecurity posture by following the third principle of the "Charter of Trust": manage the ecosystem. Founded in 2018 at the Munich Security Conference, the Charter of Trust (CoT) was initiated by Siemens to join forces with partner companies safeguarding society and businesses against the increasing exposure to malicious cyberattacks. Together with CoT partners and service providers such as TÜV SÜD, OneTrust and Panorays, Siemens tested various approaches to ensure adherence to a set of baseline requirements for supply-chain security.

After a global announcement, more partners joined the test phase from November 2021. This initiative identified external service providers and laid the groundwork for enhanced transparency and scalability within Siemens' supply chain. Challenges in stakeholder identification and in convincing providers to tailor solutions were overcome with a gradual approach, starting with pilot assessments.

The key takeaway emphasizes the pivotal role of partnering with an extended partner ecosystem for ensuring sustained success in cybersecurity resilience across the supply chain.



CASE STUDY 15

Arçelik

Balancing security with operational efficiency

Providing remote access to suppliers in a manufacturing environment can be challenging due to the presence of multiple vendors and the diverse operational landscape. Ensuring that security solutions do not disrupt daily operations or production further adds to the challenge.

Arçelik implemented a new method for secure third-party remote access. This method uses a single file that eliminates the need for additional VPN (virtual private network) connections or organizational user accounts, which enhances operational efficiency. Each unique file is created with one-time access authorization and can be shared through a file-sharing channel.

This solution offers several security benefits. It allows Arçelik to record remote access logs, which provides a clear record of activity. Additionally, it restricts manoeuvres that could escalate privileges, further protecting the system. Overall, this approach prevents security problems that can arise from traditional third-party remote access applications used for stakeholders' remote access.

Arçelik took a proactive step towards securing supplier access across its 22 factories while prioritizing production continuity. More than 50 third-party remote access applications out of 58 have been blocked from the Arcelik environment that has more than 25,000 devices.

CASE STUDY 16

Dragos and Rockwell Automation

Evaluating supply-chain cybersecurity measures

Dragos observed 50 ransomware groups impacting industrial organizations in 2023 (up 28% in 2022) and 905 ransomware incidents impacting industrial organizations (a 49.5% increase). Manufacturing was impacted the most, in 71% of ransomware incidents. Trend Micro's "What Decision-Makers Need to Know About Ransomware Risk" found 69% of ransomware attacks by the cybercriminal group Conti and 80% by the threat actor Lockbit impacted organizations with under 500 employees.

Ransomware risk is high for small and medium manufacturing organizations. This impacts customers: multiple large manufacturers shut down plants when a critical supplier is hit with ransomware.

After multiple small and medium suppliers informed Rockwell Automation they were impacted by ransomware and couldn't deliver products for at least a month, Rockwell launched a new initiative. They assessed cybersecurity in their top 50 critical suppliers, finding small suppliers had little cybersecurity and medium suppliers had some in IT but not OT. They started a multi-year initiative to educate suppliers on cybersecurity and made cybersecurity contractually required. They are extending this initiative to OT cybersecurity using free resources from Dragos OT-CERT.

The result has been a dramatic improvement in Rockwell's end to end supply-chain operations resiliency, customer protection, delivery times, company revenue and reputation. Significant improvement in cyber culture and awareness of the need to protect digital systems with proper security hygiene is a new standard for Rockwell suppliers and is now part of doing business with the company.

CASE STUDY 17

Volkswagen Group

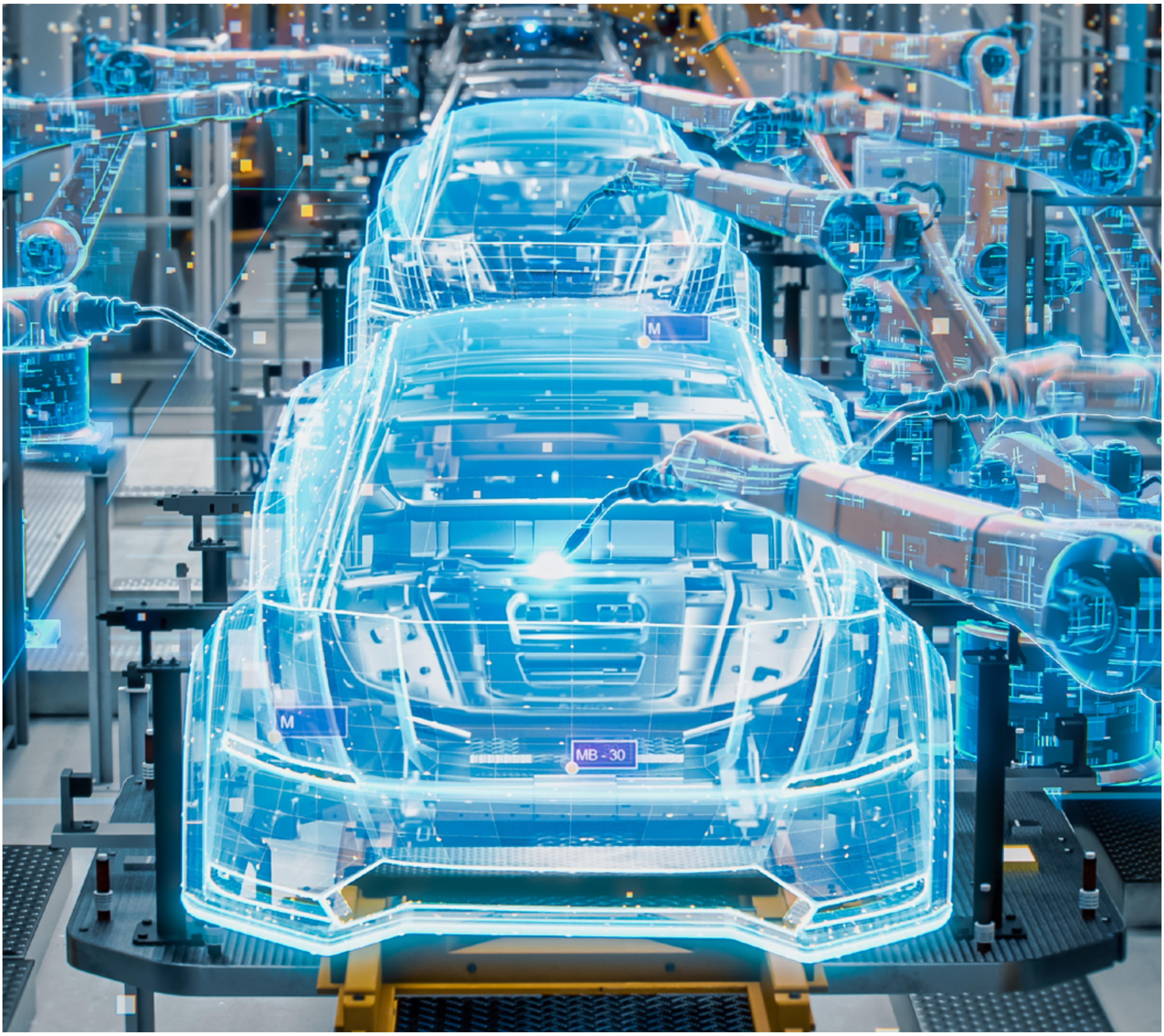
Leveraging cybersecurity requirements for production

In the realm of industrial cybersecurity, Volkswagen Group's industrial control systems and production planning departments have jointly developed two applicable documents (also knowns as MgUs – mitgeltende Unterlagen), outlining cybersecurity requirements for suppliers in procurement and production phases.

- The first document focuses on IT security requirements for systems and components within production environments. It defines essential standards on information and IT security for the release of components and systems.
- The second document addresses IT security within production plants, delineating requirements for information security during the procurement and integration of new manufacturing plants, machinery and related infrastructure, including necessary tools like IT equipment.

Compliance with both documents is mandatory and the requirements are also enshrined in Volkswagen's industrial cybersecurity guidelines, which stipulate that Volkswagen's information security requirements must be adhered to during planning and construction phases of plants and systems as well as during component selection and procurement.

These requirements are aligned with current IT security best practices, and manufacturers are required to incorporate IT security considerations into their development processes.



Conclusion

As digitalization opens avenues to enhance efficiency, productivity and competitiveness, it becomes increasingly crucial for the manufacturing sector to prioritize the development of a robust cyber resilience culture. This is essential to effectively navigate the growing landscape of cyberthreats.

A holistic cyber resilience culture enables manufacturers to maintain consistent and resilient operations, effectively addressing digital challenges while ensuring business efficiency. Integrating cyber resilience into business strategies is fundamental to enable manufacturing organizations to fully leverage the transformative potential of digitalization and innovation.

To successfully establish and maintain a cyber resilience culture in the manufacturing sector, continuous collaborative efforts across all stakeholders are imperative. The World Economic Forum's Centre for Cybersecurity and Centre for Advanced Manufacturing and Supply Chains will continue their shared efforts to engage leaders across industry sectors as well as governments, academia and civil society to raise awareness and incorporate these principles into their overall strategies. Towards that end, the Forum endeavours to share the cyber resilience principles and encourage their adoption in multiple ways, such as through the Global Lighthouse Network.[36]

In addition, the Forum is working in a cross-industry effort to solve complex and systemic cyber resilience challenges for industries including the critical group of small and medium enterprises.[37] As the human factor is critical for cultural change and with 52% of organizations lacking the right resources, the Forum is developing actions to bridge this cyber skills gap.[38]

Recognizing the complexity and scale of integrating cyber resilience across the manufacturing ecosystem, this playbook offers guidance to understand the impact of cyber risk on manufacturing and work together to drive a successful cyber resilience culture in manufacturing.

Contributors

Lead authors

Filipe Beato
Lead, Centre for Cybersecurity,
World Economic Forum

Eric Enselme
Executive Fellow, Centre for Advanced
Manufacturing and Supply Chains,
World Economic Forum

Giulia Moschetta
Research and Analysis Specialist,
Centre for Cybersecurity, World Economic Forum

Advisory group

Kiva Allgood
Head, Centre for Advanced Manufacturing and
Supply Chain, World Economic Forum

Akshay Joshi
Head of Industry and Partnerships,
Centre for Cybersecurity, World Economic Forum

Acknowledgements

This playbook was co-created with cyber and supply leaders from diverse organizations as part of the World Economic Forum's Cyber Resilience in Manufacturing community. The individuals contributed with thought leadership, shared insights and lessons learned and participated in workshops and consultation sessions. The World Economic Forum would like to thank the following individuals for their leadership, insightful contributions and feedback.

Mansur Abilkasimov, Schneider Electric

Omkhar Arasaratnam, Linux Foundation

Tony Baker, Rockwell Automation

Stefan Braun, Henkel

Emre Bilgili, Arçelik

Daniel Bren, OTORIO

Dawn Cappelli, Dragos

Ruben D. Chacon, Eaton Corporation

Paul Champkin, Unilever

Piotr Ciepiela, EY

Younes Dragoni, Global Shapers

Walid El-Khazen, Kuwaiti Danish Dairy (KDD)

Vijay Fernandes, Kuwaiti Danish Dairy (KDD)

Richard Hale, Sony Group

Eram Hasan, Engro Corporation

Cynthia Hutchison, US Center for Advanced Manufacturing (Centre for the Fourth Industrial Revolution)

Andreas Kind, Siemens

Katelyn Kontny, Automation Alley

Ryan Lasmaili, Vaultree

Kris Lovejoy, Kyndryl

Garima Maheshwari, Johnson & Johnson

Vasu Modekurti, Underwriters Laboratories

Mark Orsi, Global Resilience Federation

Tom Parker, Hubble Technology

Del Rodillas, Palo Alto Networks

John Schilling, Rockwell Automation

Christina-Dorothea Schlichting, Volkswagen

Karan Sondhi, Trellix

Frédéric Thomas, Kudelski Group

Ian Tien, Mattermost

Ersin Uslu, Eczacıbaşı Holding

Salvador E. Venegas-Andraca, Tecnológico de Monterrey

Friedrich Wetschnig, FLEX

Ryan Whelan, Our Next Energy

Mike Wilkes, New York University

Lars Zywietz, Accenture

The Forum also wishes to acknowledge contributions from Trevor Rudolph and Dee Kimata from Schneider Electric, Kristy Paine from Splunk, Brecht Wyseur from Kudelski, and from Roger Hill.

Production

Bianca Gay-Fulconis
Designer, 1-Pact Edition

Tanya Korniichuk
Illustrator, 1-Pact Edition

Madhur Singh
Editor, World Economic Forum

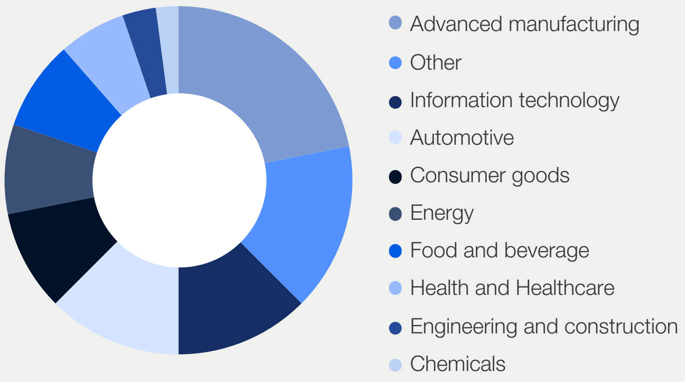
Methodology

For this paper, the World Economic Forum gathered insights from three sources all through 2023 and 2024. These included:

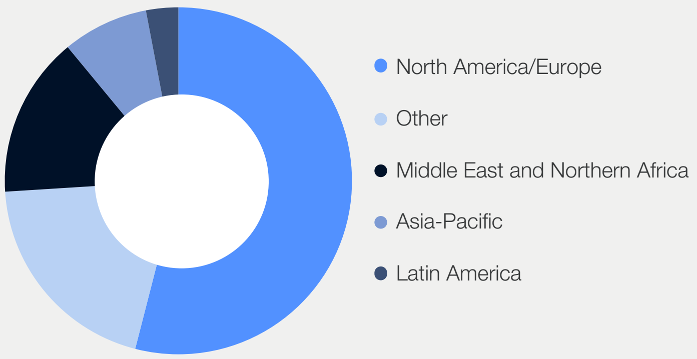
- Regular community workshops: 10 virtual and one in-person roundtable gathered more than 30 members to discuss, align and collect insights to define the guiding principles to build a culture of cyber resilience in manufacturing.
- Bilateral consultations with community members and sector leaders were also conducted to gain further insight into the challenges and opportunities.
- Insight gathering survey: The survey was conducted between December 2023 and February 2024 to collect insights on cyber resilience in manufacturing. The survey gathered more than 100 responses from cyber leaders and business executives from manufacturing organizations on: the industry, organization size and location, cybersecurity reporting line, cyberthreats, cyber incident impact and challenges. The data collected is anonymous and not attributable to any single person or entity.

All the discussions were held under Chatham House rules; consequently, no information in this report is attributed to a specific member.

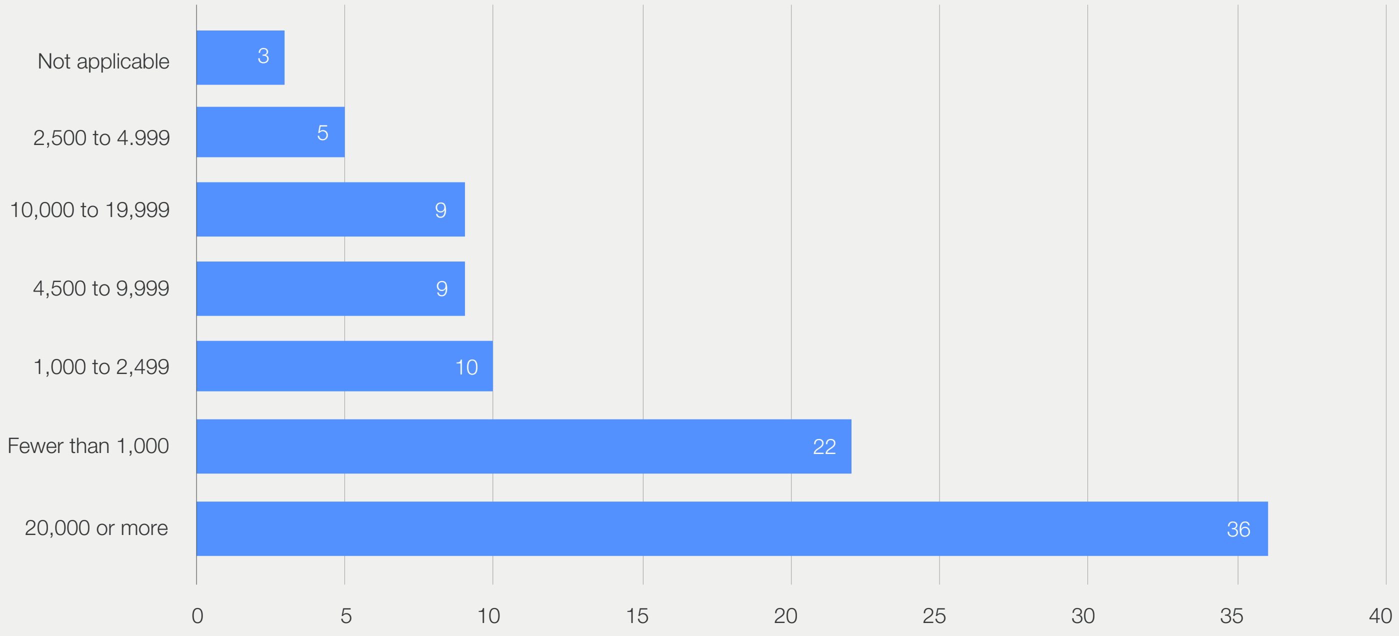
Survey industry sample (%)



Geographical diversity of survey responders (%)



Survey responders’ organization size (%)



Endnotes

1. Deloitte. (2024). *2024 Manufacturing Industry Outlook*. https://www2.deloitte.com/us/en/insights/industry/manufacturing/manufacturing-industry-outlook.html
2. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.
3. IBM. (2024). *IBM X-Force Threat Intelligence Index 2024. IBM Security X-Force Threat Intelligence Index 2024*.
4. Dragos. (2024). *2023 OT Cybersecurity Year in Review*. https://www.dragos.com/ot-cybersecurity-year-in-review/.
5. Waterfall Security. (2023) *2023 Threat Report – OT Cyberattacks With Physical Consequences*. https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2023-threat-report-ot-cyberattacks-with-physical-consequences/.
6. McKinsey. (2024). *Boards of directors: The final cybersecurity defense for industrials*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/boards-of-directors-the-final-cybersecurity-defense-for-industrials?stcr=F0BA7BB4F85F43F292A925704DDA0AFB&cid=other-eml-alt-mip-mck&hlkid=5b12ca08acb54a65a6a159820bdff781&hctky=12004288&hdpid=7ad4a147-b8b8-46d8-8763-14d759425e48#/.
7. Chainalysis. (2024). *2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.
8. More information on survey methodology available in appendix.
9. Dragos. (2024). *OT Cybersecurity: The 2023 Year in Review*. https://www.dragos.com/ot-cybersecurity-year-in-review/.
10. Ibid.
11. ENISA. (2023). Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
12. NIST. (2024). *Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary.
13. Abilkasimov,M., Dawn, C., Beato, F. and Moschetta, G. (2023). *Manufacturing is the most targeted sector by cyberattacks. Here's why increased security matters*. World Economic Forum. https://www.weforum.org/agenda/2023/03/why-cybersecurity-in-manufacturing-matters-to-us-all/.
14. World Economic Forum. (2024). *Global Cybersecurity Outlook*. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.
15. Recorded Future. (2024). *Plant production still on hold for German battery manufacturer after cyberattack*. https://therecord.media/varta-battery-plant-production-on-hold-after-cyberattack.
16. Recorded Future. (2023). *Semiconductor industry giant says ransomware attack on supplier will cost it $250 million*. https://therecord.media/applied-materials-supply-chain-mks-ransomware-attack.
17. Reuters. (2022). *Toyota suspends domestic factory operations after suspected cyberattack*. https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/.
18. ISC2. (2023). *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf.
19. Microsoft. (2022). *Secure your OT and IoT devices with Microsoft Defender for IoT and Quzara Cybertorch™*. https://www.microsoft.com/en-us/security/blog/2022/03/03/secure-your-ot-and-iot-devices-with-microsoft-defender-for-iot-and-quzara-cybertorch/.
20. OpenSSF. (2024). *OpenSSF and CISA Join Forces to Secure Open Source Software*. https://openssf.org/blog/2024/03/07/openssf-and-cisa-join-forces-to-secure-open-source-software/.
21. Ibid.
22. Wired. (2024). *The XZ Backdoor: Everything you need to know*. https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/.
23. CISA. (2023). *Cross-Sector Cybersecurity Performance Goals*. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.
24. U.S. Securities and Exchange Commission. (2023). *Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures*. https://www.sec.gov/news/press-release/2023-227.
25. International Society of Automation. (2024). *ISA/IEC 62443 Series of Standards*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.
26. Directors & Boards. (2024). *Manage Cybersecurity as Part of the ESG Strategy*. https://www.directorsandboards.com/board-issues/cyber-risk/manage-cybersecurity-as-part-of-the-esg-strategy/.
27. SANS (2022). *The Five ICS Cybersecurity Critical Controls*. https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/.

28. World Economic Forum. (2021). *Principles for Board Governance of Cyber Risk*. https://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf.

29. NIST. (2024). *Cybersecurity Framework 2.0*. https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft.

30. World Economic Forum. (2021). *Principles for Board Governance of Cyber Risk*. https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/.

31. NIST. (2024). *Computer Security Resource Center Glossary*. https://csrc.nist.gov/glossary.

32. SANS (2022). *The Five ICS Cybersecurity Critical Controls*. https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/.

33. World Economic Forum. (2023). *Unlocking Cyber Resilience in Industrial Environments: Five Principles*. https://www.weforum.org/publications/unlocking-cyber-resilience-in-industrial-environments-five-principles/.

34. NIST. (2024). *Cybersecurity Framework 2.0*. https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft.

35. World Economic Forum. (2023). *Unlocking Cyber Resilience in Industrial Environments: Five Principles*. https://www.weforum.org/publications/unlocking-cyber-resilience-in-industrial-environments-five-principles/.

36. World Economic Forum. *Global Lighthouse Network*. https://initiatives.weforum.org/global-lighthouse-network/.

37. World Economic Forum. *Cyber Resilience in Industries*. https://initiatives.weforum.org/cyberresilienceindustries/.

38. World Economic Forum. *Bridging the Cyber Skills Gap*. https://initiatives.weforum.org/bridging-the-cyber-skills-gap/.

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org