built to defend

SMART & SECURE: WHY SMART FACTORIES NEED TO PRIORITIZE CYBERSECURITY

#GetTheFutureYouWant

Capgemini
RESEARCH INSTITUTE

Executive Summary

As cyberattacks have grown in both frequency and intensity in recent years, the smart factory has become a prominent potential target. Smart factories, by their nature, need to be connected to cloud or the internet; while this instant global network connection brings a plethora of communicative advantages, it also results in a significant increase in the surface area vulnerable to attack via digital means.

However, awareness of the mounting risks does not necessarily translate to preparedness on an organizational level. Many organizations we surveyed say their cybersecurity analysts are overwhelmed by the vast array of Operations Technology (OT) and Industrial Internet of Things (IIOT) devices they must track in their attempts to discover and disable attempted breaches of their security.

+

In our survey, we found that:

80% of organizations agree that cybersecurity is a critical component of a smart factory

79% organizations feel cyber-risk is higher in a smart factory than in traditional/non-smart factories.

Executive Summary

We found organizations in general to be inadequately prepared in terms of **awareness, governance, protection, detection,** and **resilience.** Our analysis indicates that governance is a particular area of concern, with this area demonstrating the lowest level of preparedness across multiple parameters.

+ Key challenges in bringing smart-factory cybersecurity up to speed

Lack of collaboration between smart factory leaders and the Chief Security Officer

Inadequate proportion of the annual budget channeled to cybersecurity

Failure to detect cyberattacks early leading to a higher level of damage being inflicted on their operations

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Executive Summary

We found that a subset of our sample had established mature practices of cybersecurity: awareness, preparedness, and implementation of cybersecurity in smart factories. We found that these mature organizations outperform their peers in multiple aspects of cybersecurity: 74% of "'Cybersecurity Leaders" can recognize known attack patterns (e.g., those used by the WannaCry and NotPetya malware) at an early stage in their deployment, compared to just 46% of other organizations. Eighty percent of Cybersecurity Leaders can respond to cybersecurity threats in their smart factories, compared to only 51% of the rest. Moreover, 72% of Leaders can mitigate and reduce the impact of cybersecurity attacks on their smart factories, compared to only 41% of other organizations.

The following steps can help organizations to be better prepared to prevent and mitigate cyberattacks:

- perform an initial cybersecurity assessment of the whole organization;
- build awareness of smart-factory cyberthreats across the organization;
- identify risk ownership for cyberattacks in smart factories;
- establish a framework that monitors and facilitates smart-factory cybersecurity;
- embed cybersecurity practices tailored to the smart-factory environment;
- establish strong governance structures with rigorous oversight measures.

80%

of organizations agree that cybersecurity is a critical component of a smart factory

Definitions

+ Smart factories

Three key digital technologies enable smart factories to optimize productivity, flexibility, and quality of service:

• connectivity (utilizing the Industrial Internet of Things (IIOT) to collect data from existing equipment that has been enhanced by new sensor technology);
• intelligent automation (e.g., advanced robotics, machine vision, distributed control, drones, etc.);
• cloud-based data management and analytics (e.g., predictive analytics/AI).

+ Cybersecurity in smart factories

This research looks at cybersecurity from an intelligent-manufacturing and smart factories perspective. Cybersecurity in smart factories encompasses all measures needed to secure the shop floor, as well as facilities management; security systems (physical-access control); IIOT; and edge computing connected to cloud. Cybersecurity

covers systemic defense across identification, protection, discovery, response, and recovery relating to cyber threats. We have included in this research both new, purpose-built smart factories and existing manufacturing plants that have been modified to achieve smart-factory status.

Definitions

+ Cyberattack*

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information

+ Cyberthreat*

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

+ Cyber Risk*

An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.

*Source: National Institute of Standards and Technology, US Department of Commerce.

Introduction

Cyberattacks have become a global menace. Ill-prepared organizations live in fear of their operations being slowed or even frozen while they are faced with steep ransom demands that must be fulfilled before the attacker permits operations to resume. To exacerbate the threat, it seems that the cyberattack "sector" is immune both to global pandemics and their related recessions. Despite the slowdown of global business in the face of COVID-19, cyberattacks continued to occur at a steady rate (73% of organizations that had suffered an attack on their smart factories said that it had taken place within the past 12 months). Widespread digitization has made smart factories the new frontier of cyberwarfare; due to the spread of smart factories, by 2025 the count of Industrial Internet of Things (IIoT) connections is expected to reach 37 billion.[1] Nearly 68% of organizations have already begun implementation of a smart-factory initiative.[2]

Organizations across the world are recognizing the importance of securing their manufacturing operations against a potential cyberattack. Global consumer product company Unilever, for example, has focused on factory cybersecurity during the pandemic: it is building a registry of digital assets for each of its more than 300 plants, as well as scanning its existing system for vulnerabilities that need to be eradicated. Unilever is also working to insulate its plants' digital-technology networks within the company's systems, so that the impact of an attack can be isolated at factory-floor level, protecting the rest of the manufacturing facility and the corporate network.[3]

Takeda Pharmaceutical Company, an American-Japanese multinational pharmaceutical manufacturer seeking to become an industry leader in healthcare information security, is currently preparing to invest in its cybersecurity system. It is also collaborating with partners to create a secure ecosystem in which they can immerse their manufacturing and supply-chain operations.[4]

Introduction

To understand how organizations are securing their smart factories and the challenges they must overcome to do so, we surveyed 950 organizations globally. The sectors we surveyed include heavy industry, pharma and life sciences, chemicals, hi-tech, consumer products, automotive, and aerospace and defense. We also conducted one-on-one interviews with a range of senior cybersecurity officers across sectors.

+

The key questions that this research seeks to answer are:

01

Why are smart factories the new frontier in cyberspace?

02

What is the general level of preparedness of smart factories in terms of cybersecurity?

03

What are the key challenges to implementing smart-factory cybersecurity initiatives?

04

How can organizations ensure robust cybersecurity for their smart factories?

01

Smart factories: The new frontier in cyberspace

40% of organizations have been victim of a cyberattack
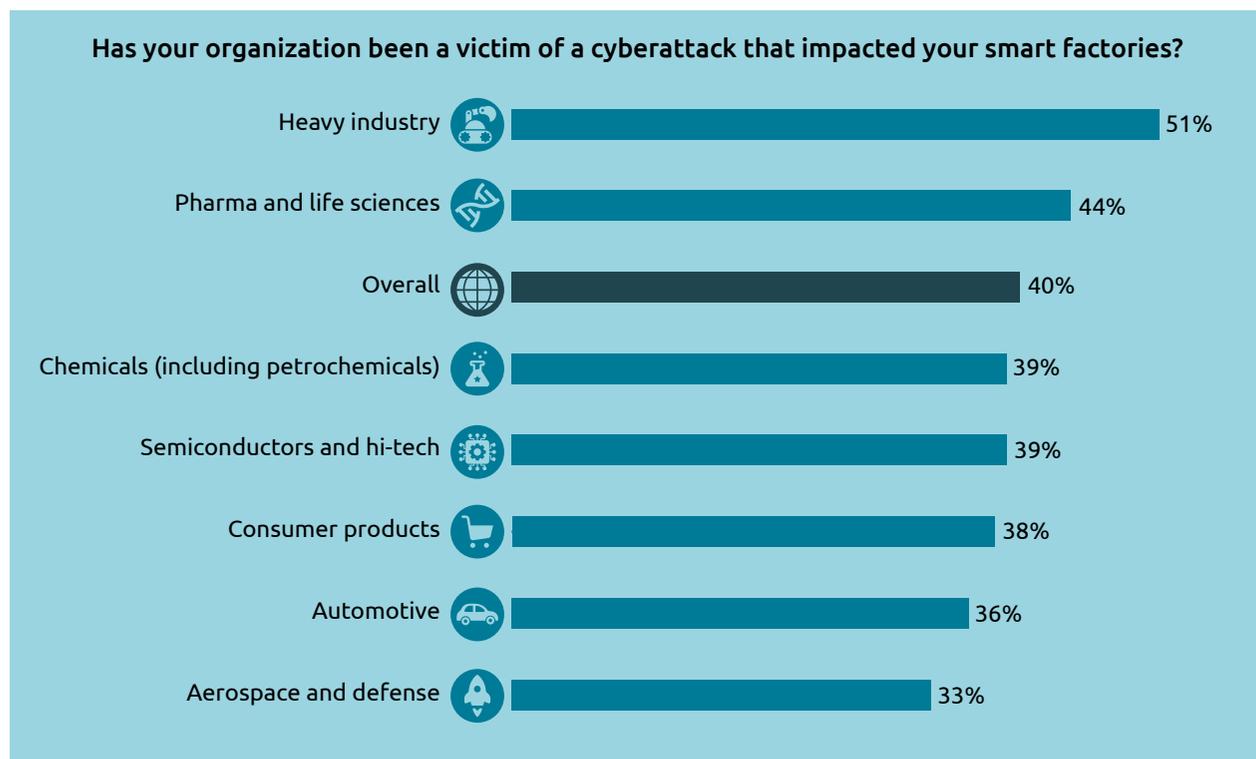that impacted their smart factories

Smart factories are increasingly being targeted by cyberattacks

Nearly 68% of organizations in our survey confirmed that they have ongoing smart-factory initiatives.[5] With the smart factory being one of the emblematic technologies of the transition to digitization, it is also a prime target for cyberattackers, 40% of organizations surveyed have been victim of a cyberattack that impacted their smart factories (Figure 1). Among sectors, heavy industry faced the highest volume of cyberattacks (51%). Half of UK manufacturers said they have been targeted, with nearly one-quarter suffering losses of £5,000–25,000, and 6% losing £100,000 or more.[6]

Since 2019, organizations have seen an increase in various forms of cyberattack: 27% of firms who were impacted have seen an increase of 20% or more in hackers infiltrating unsecured IIOT devices for distributed denial-of-service (DDoS) attacks. Attacks can also come, wittingly or unwittingly, from the inside: 28% of firms who were impacted have seen an increase of 20% or more in employees or vendors bringing in infected devices, such as laptops and handheld devices, to install/patch smart-factory machinery.

Has your organization been a victim of a cyberattack that impacted your smart factories?

Sector	%
Heavy industry	51%
Pharma and life sciences	44%
Overall	40%
Chemicals (including petrochemicals)	39%
Semiconductors and hi-tech	39%
Consumer products	38%
Automotive	36%
Aerospace and defense	33%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Most organizations have suffered a smart-factory cyberattack in the past 12 months

As many as 73% of organizations that said they had suffered an attack mentioned that it had taken place during the previous 12 months, 13% within the previous 12–24 months, and 14% had faced a cyberattack more than 24 months ago (Figure 2). Overall, 40% of organizations reported an increase in cyber incidents since 2019. A Head of Cyber Security Service Operation Center at a large European defense firm underlines this: *"In the past two years, the needs of cybersecurity in OT [operational technology] and IT [information technology] have been growing as the frequency of attacks has risen."*

A cybersecurity lead at a major automotive OEM based in India confirms this: *"All the security controls, such as maintenance and security-patch updates, are performed regularly by IT but, since the OT machines have a legacy system and hackers also want real-time information from the machines, hackers are changing the attack vector from IT to OT."*
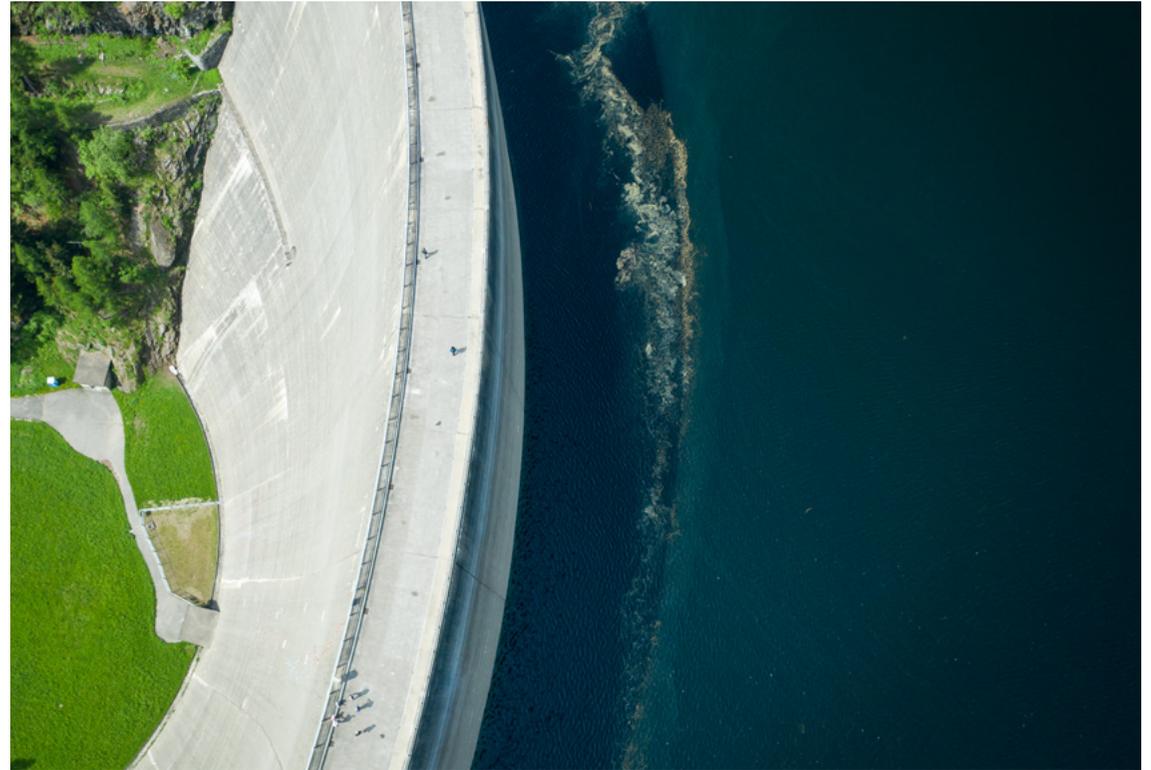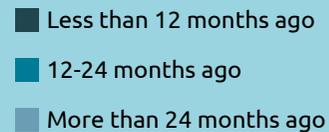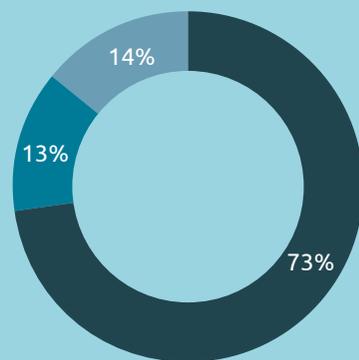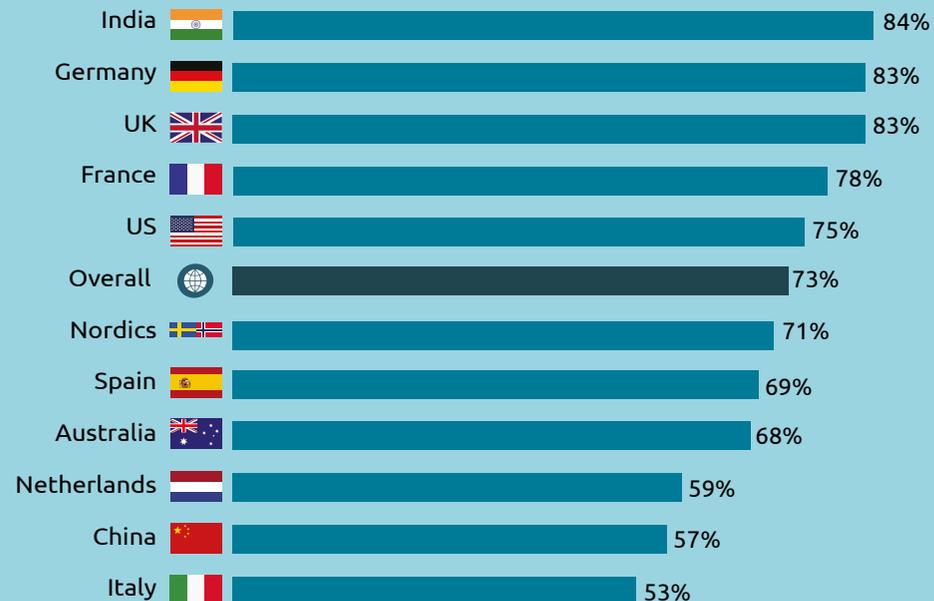
Fig.2

Most organizations impacted by cyberattacks said they took place in the past 12 months

When did the last cyberattack take place?

- 73%
- 13%
- 14%

- ■ Less than 12 months ago
- ■ 12-24 months ago
- ■ More than 24 months ago

Last cyberattack took place less than 12 months ago

India	84%
Germany	83%
UK	83%
France	78%
US	75%
Overall	73%
Nordics	71%
Spain	69%
Australia	68%
Netherlands	59%
China	57%
Italy	53%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations

Why are attacks on smart factories becoming more frequent?

Traditional factories, which are physically and technologically closed entities that are not connected to IT networks, are easier to secure against cyberattack. With smart factories, which use a greater implementation of IIOT devices, complete security is impossible given the significantly enlarged attack surface area. By 2025, due to the proliferation of smart factories, the number of IIOT connections is expected to reach 37 billion.[7]

Moreover, majority of organizations do not have systemic visibility of the OT/IIOT devices at their smart-factory locations. The machinery is usually comparatively old, and may have been designed at a time before cybersecurity was considered a key element of the design process. System-level visibility of devices is essential to detecting when they have been compromised. In any case, as a tenet of good practice, regular system-risk assessments are useful in helping to prevent attacks; however, not all organizations conduct these. This may be because organizations cannot scan machines at a smart factory/ manufacturing location during operational uptime (an issue mentioned by 45% of organizations).

The Global CISO at an international personal-hygiene group adds: *"A plant manager is responsible for making sure that their machinery produces the goods at an agreed rate, to a high standard. To patch a machine or deploy an update, we need to take that machine offline."*

"With smart factories, complete security is impossible given the significantly enlarged attack surface area"

Graham Thomson, CISO at Irwin Mitchell, a legal firm that specializes in cybersecurity issues, elaborates: *"Say a company installs a new HVACS [heating, ventilation, and air-conditioning] system, but they don't realize it is accessible via the internet. If password-protection is not set up securely, the system can easily be accessed remotely. A hacker can play with the settings, making conditions too hot or cold to work efficiently, or possibly even use this system to access other internal IT systems. It's a very effective impact from a simple intervention. We regularly see simple methods like a USB stick breach the air gap."*[8]

Organizations are aware of the smart-factory cyberthreat – but don't always act

Around 53% of organizations – including 60% of heavy-industry organizations – agree that most future cyberthreats will feature smart factories as their primary targets. However, a high level of awareness and a vague sense of dread does not automatically translate to high preparedness.

Manoj Nair, Head of IT at Continental Automotive India, an automotive parts manufacturing company, emphasizes the danger to the manufacturing sector: *"Nearly any process in manufacturing can be subject to a breach in security, especially considering the level of connectivity in modern manufacturing settings. As a result, manufacturers must 'think outside the box' to assess and identify cybersecurity threats."*[9]
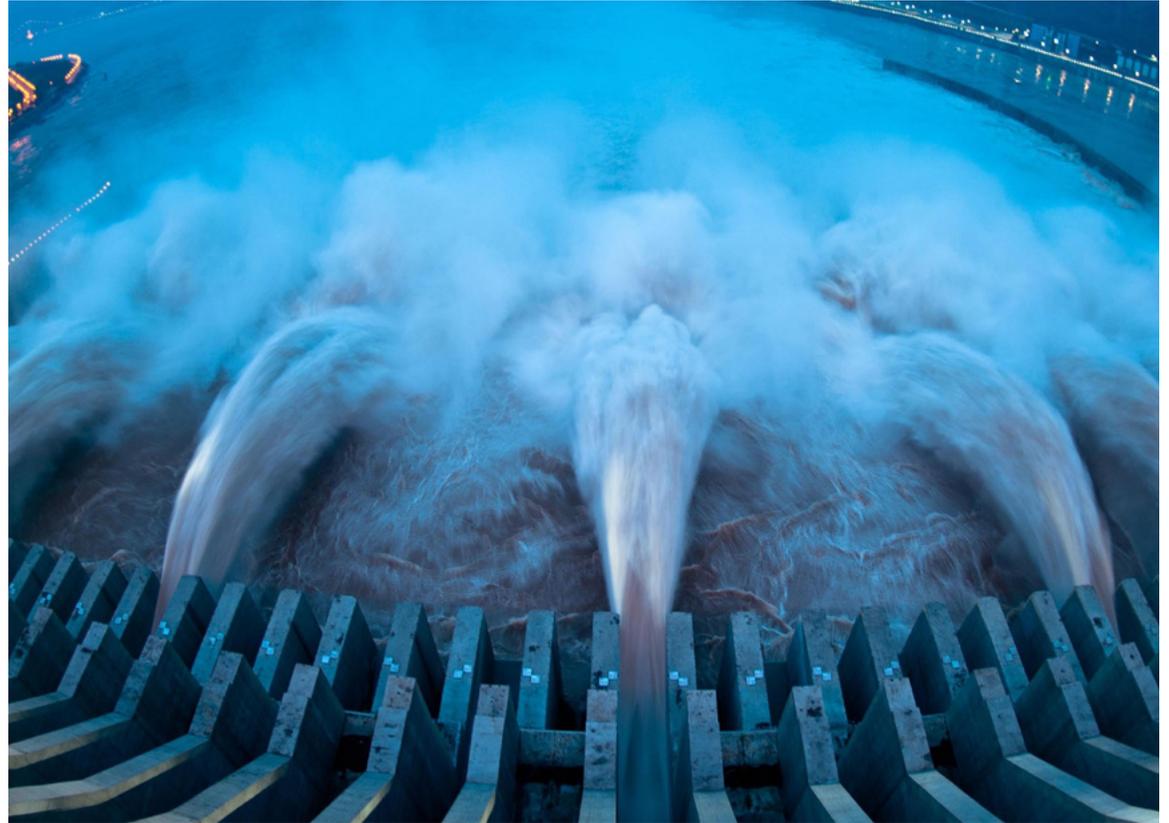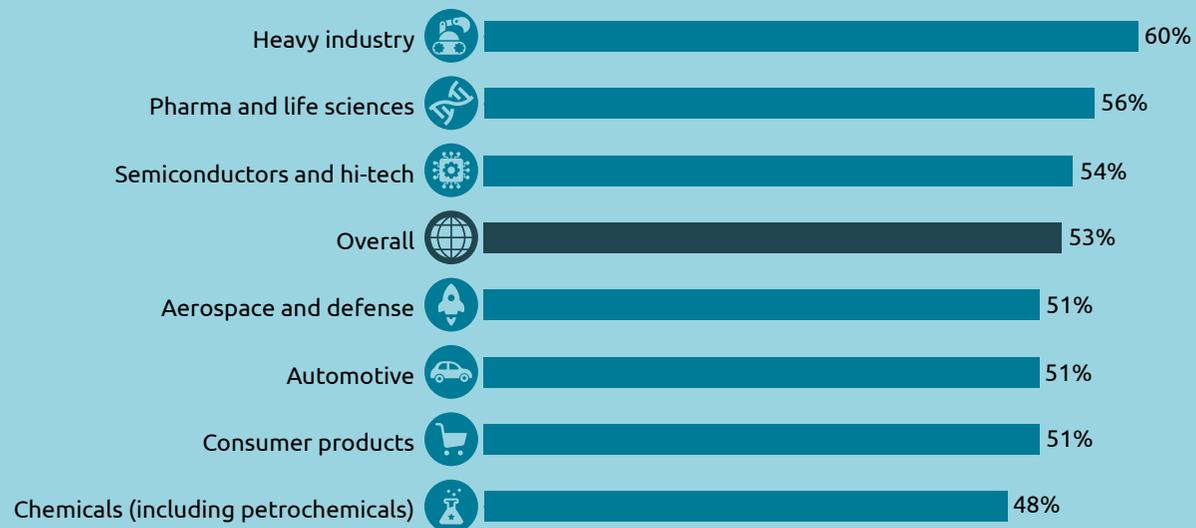
53%

of organizations – including 60% of heavy-industry
organizations – agree that most future cyberthreats will
feature smart factories as their primary targets.

Organizations are aware that most future cyberthreats will target smart factories - by sector

Sector	Percentage
Heavy industry	60%
Pharma and life sciences	56%
Semiconductors and hi-tech	54%
Overall	53%
Aerospace and defense	51%
Automotive	51%
Consumer products	51%
Chemicals (including petrochemicals)	48%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

How are organizations securing their smart factories

Detection

Unilever is working on a multi-year framework plan to:
- Build a registry of digital assets for each plant and identify vulnerabilities.
- Insulate digital technology networks within broader plant systems to prevent attacks spreading from the factory floor throughout the organization.[1]

Assessment

Chevron is working on:
- Automating and scaling its OT cyber assessments and intelligent insights to improve and augment cybersecurity.
- Bringing consistency to performance metrics and reports, enabling the organization to track improvements and measure program effectiveness with greater accuracy.[2]

Monitoring

Taro Pharmaceuticals has implemented:
- A network-monitoring solution specifically designed to secure connected OT environments.
- This affords it full visibility of its network, reducing operational downtime and improving network security.[3]

Sources:

1. The Wall Street Journal, "Unilever focuses on factory cybersecurity as pandemic sparks run on consumer staples," December 2020.
2. PRN News, "SecurityGate.io selected by Chevron to help them scale global OT cybersecurity," September 2020.
3. SCADAFence, "Pharmaceuticals like Johnson & Johnson are experiencing daily cyber attacks from nation state attackers," April 2021.

02

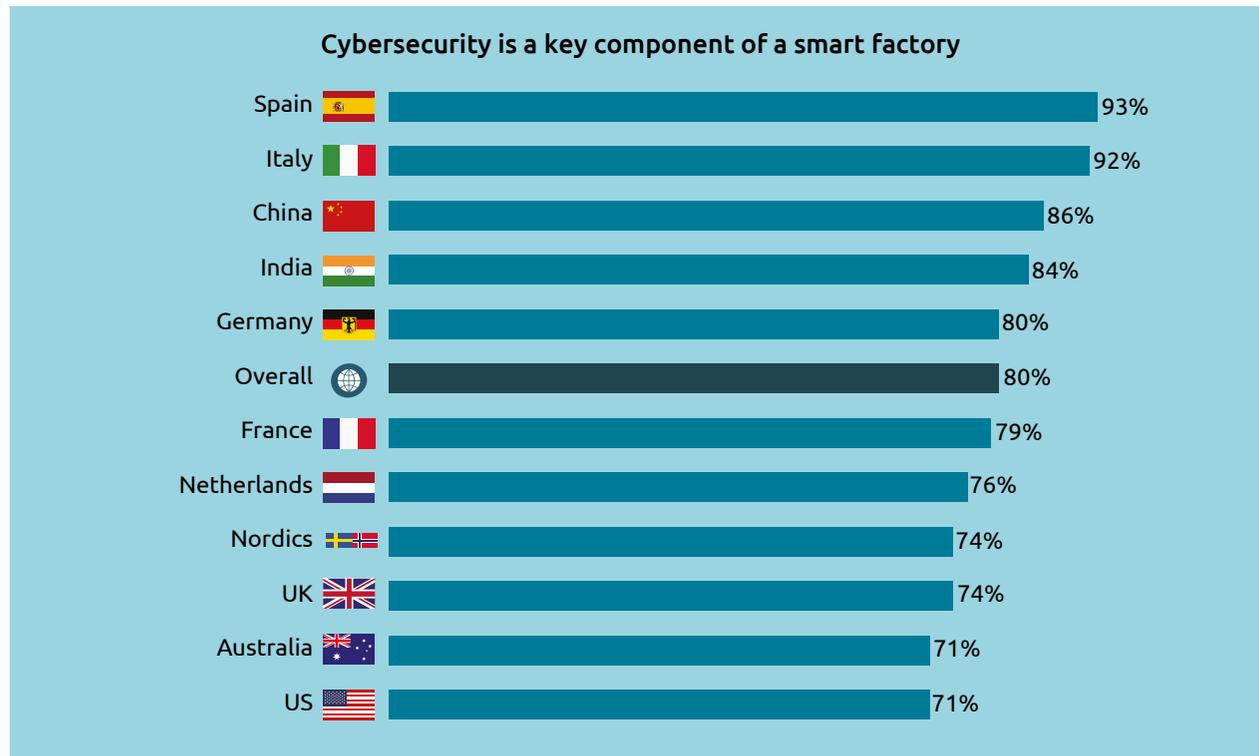# Cyberthreat awareness is not the same as preparedness

Fig.4

Most organizations agree cybersecurity is key

Organizations agree that cybersecurity is a critical component of smart factories

Fully 80% of organizations agree that cybersecurity is a critical component of a smart factory's operations and 79% of organizations feel that the level of cyberthreat is higher in a smart factory than in a traditional, non-connected factory. Although 51% of organizations acknowledge that the number of cyberattacks is likely to increase over the next 12 months, current levels of preparedness are low. The Global CISO at an international personal-hygiene group adds: *"The risks to the business from cyberattacks are: intellectual property theft, operational disruption, low product quality, and plant closure. Safety of workers is also compromised as cyberattacks could injure operators."*

Cybersecurity is a key component of a smart factory

Country	Percentage
Spain	93%
Italy	92%
China	86%
India	84%
Germany	80%
Overall	80%
France	79%
Netherlands	76%
Nordics	74%
UK	74%
Australia	71%
US	71%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

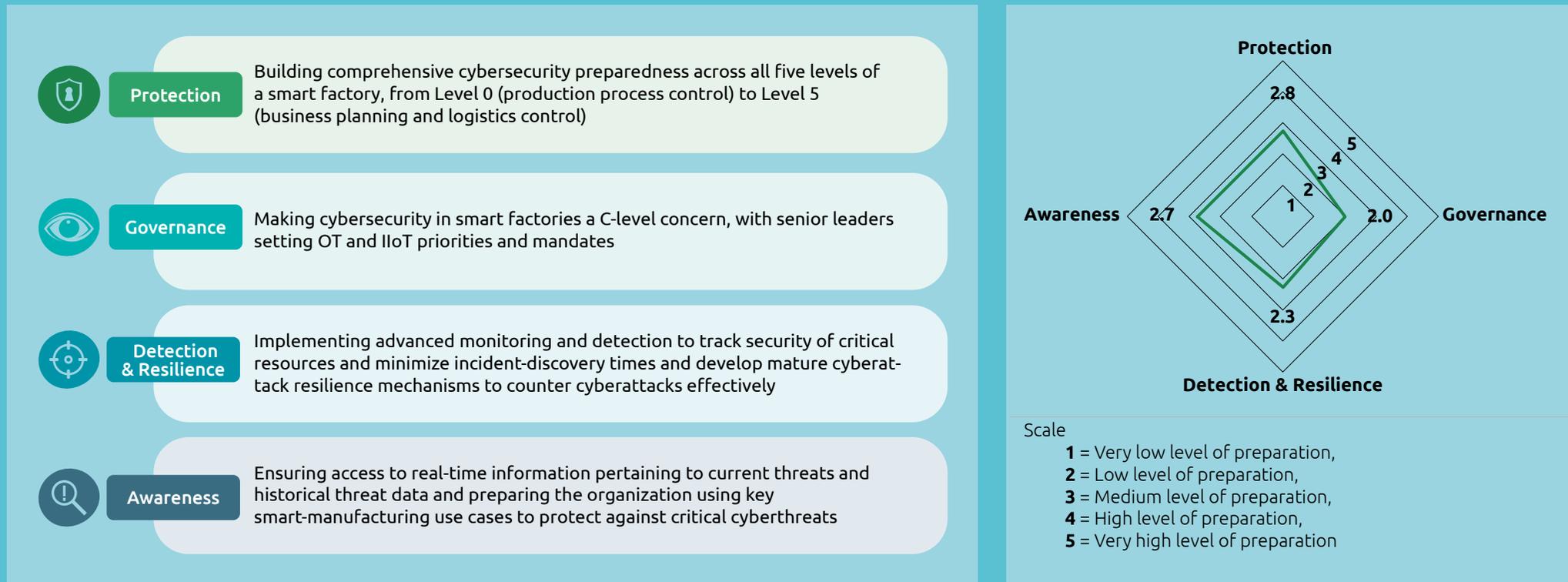## Organizations are not prepared enough for cyberattacks

For multiple facets of cybersecurity in smart factories, however, cyberthreat awareness does not translate to cybersecurity readiness. The Head of Cyber Security Service Operation Center at a large European defense firm adds, *"The bigger the organization, the higher the required level of cybersecurity preparedness. There is a stronger imperative for these organizations to invest in cybersecurity, as they have a bigger perimeter to defend."*

We baselined our survey responses around the dimensions of protection, governance, detection and resilience, and awareness. We next assigned a relative scoring system to arrive at a 360-degree view of an organization's cybersecurity maturity. We found that, on average, organizations have a low level of preparedness.

Fig.5

Current levels of cybersecurity preparedness are low

Protection

Building comprehensive cybersecurity preparedness across all five levels of a smart factory, from Level 0 (production process control) to Level 5 (business planning and logistics control)

Governance

Making cybersecurity in smart factories a C-level concern, with senior leaders setting OT and IIoT priorities and mandates

Detection & Resilience

Implementing advanced monitoring and detection to track security of critical resources and minimize incident-discovery times and develop mature cyberattack resilience mechanisms to counter cyberattacks effectively

Awareness

Ensuring access to real-time information pertaining to current threats and historical threat data and preparing the organization using key smart-manufacturing use cases to protect against critical cyberthreats

Scale
1 = Very low level of preparation,
2 = Low level of preparation,
3 = Medium level of preparation,
4 = High level of preparation,
5 = Very high level of preparation

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Protection

An integrated approach to ensuring the entire smart factory is connected and prepared will be essential if future cyberthreats are to be neutralized. Currently, organizations have only low preparedness across all levels of smart factories, although they may be well prepared across a few individual levels. The overall average preparedness level is only at 2.8 across all the levels, as shown in Figure 5.

Governance

Cybersecurity governance approaches for smart factories are not currently adequately integrated: many organizations say OT/IIOT and IT cybersecurity systems are not connected in their organization. One reason for this is that developing an integrated cybersecurity approach is frequently not a priority for senior management: 47% of manufacturers say cybersecurity in their smart factories is not a C-level concern. The approach of around 44% of respondents is that, if a manufacturing process is working well, it should not be touched, and there is no need to invest in smart-factory (OT/IIOT) cybersecurity. Organizations in our sample struggle with effective cybersecurity governance, scoring only 2.0 on average (see Appendix for list of requirements).

Awareness

We analyzed the preparedness of organizations for cyberattacks against key smart-manufacturing use cases and found that, for a large proportion, these use cases are not implemented on a global basis. In total, organizations scored only 2.4 in terms of having implemented all these preparedness use cases. Chevron, in an example of foresight in this regard, is working on automating and scaling its OT cyber assessments and intelligent insights to improve and augment cybersecurity. This, in turn, brings a greater measure of consistency to performance metrics and reports, enabling the organization to track improvements and measure program effectiveness with greater accuracy.[10]

It is essential that organizations gather threat intelligence to reach the optimum level of threat awareness and preparedness. Regular threat-intelligence updates improve cybersecurity preparedness of smart factories but only when analyzed effectively and acted upon promptly.
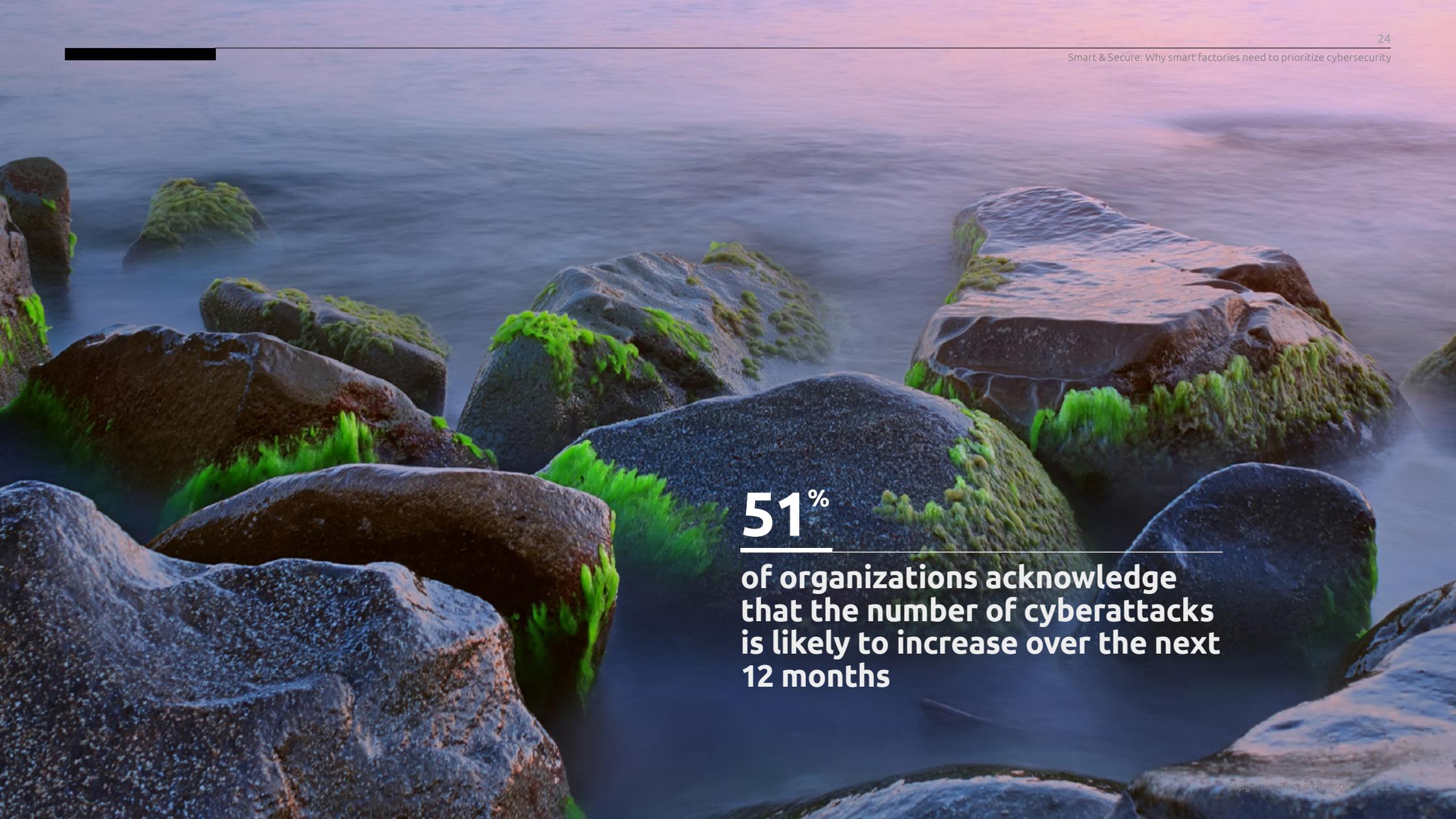
Detection and resilience

The detection of anomalous machine behavior in smart factories is key to identifying incipient cyberattacks. However, we found that not all network-connected devices are tracked and monitored by cybersecurity tools in smart factories. This leaves a vast unmonitored – and, therefore, vulnerable – attack surface for hackers to exploit. Organizations scored only 2.0 for preparedness in implementing the parameters for detection (see Appendix for list of parameters).

Organizations may be unable to investigate cyberattacks successfully in the future

Many organizations we surveyed said their cybersecurity analysts are overwhelmed by the vast array of OT and IIOT devices they must track to detect and prevent attempted intrusion. Given the recent exponential increase in the number of connected devices within smart factories, this is a problem that will only grow.

Moreover, many executives we talked to said they will be unable to respond effectively to cyberattacks in their smart factories and manufacturing locations. This impacts cybersecurity response across sectors with heavy industries, aerospace and defense being the most impacted according to executives.

51%

**of organizations acknowledge
that the number of cyberattacks
is likely to increase over the next
12 months**

Fig.6

Leaders have achieved benefits

Cybersecurity Leaders take the market advantage

We segregated the organizations in our survey sample into two segments: Cybersecurity Leaders and the rest. We define Leaders as those organizations that have mature practices across the critical pillars of cybersecurity: awareness, preparedness, and implementation of cybersecurity in smart factories.

Awareness – Awareness of organizations of potential cyberthreats originating from their enterprise and smart factory systems.

Preparedness – Preparedness of organizations against cyberattacks across key smart manufacturing components, such as plant control towers, intelligent automation, etc.

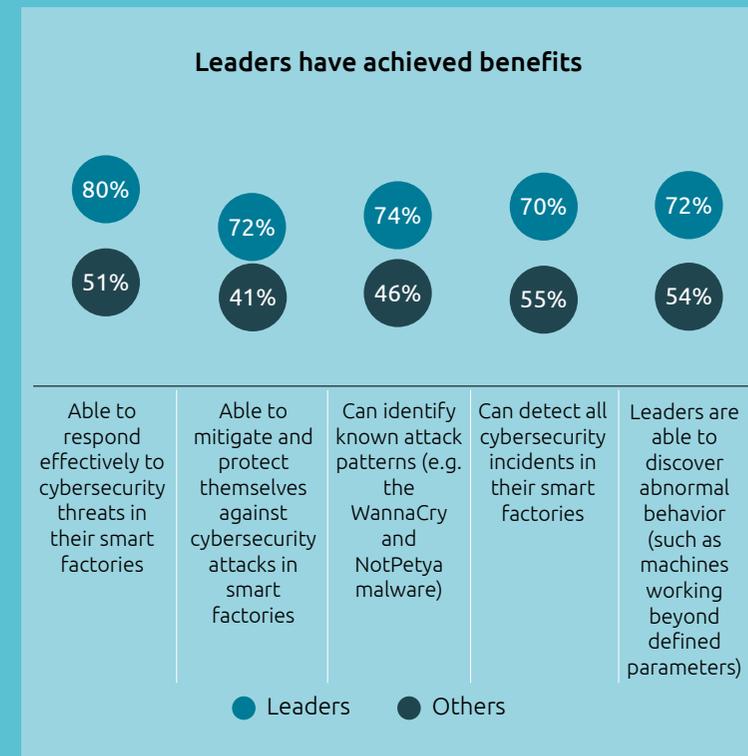**Implementation** – Maturity of organizations in key smart factory cybersecurity use cases

Based on our analysis, we identified a subset of Leaders that enjoy significant benefits. Additionally, we examined the practices and outcomes of Leaders to determine the benefits they derive. We found that these

organizations outperform their peers in multiple aspects of cybersecurity.

- **80%** of Leaders say they are able to respond effectively to cybersecurity threats in their smart factories compared to just 51% of remaining organizations;

- **72%** of Leaders say they are able to mitigate and protect themselves against cybersecurity attacks in smart factories, compared to 41% of remaining organizations;

- **74%** of Leaders can identify known attack patterns (e.g., the WannaCry and NotPetya malware), compared to 46% of other organizations;

- **70%** of Leaders believe they can detect all cybersecurity incidents in their smart factories, compared to 55% of remaining organizations;

- **72%** of Leaders are able to discover abnormal behavior (such as machines working beyond defined parameters) compared to 54% of the remaining organizations.

Leaders have achieved benefits

80%	72%	74%	70%	72%
51%	41%	46%	55%	54%
Able to respond effectively to cybersecurity threats in their smart factories	Able to mitigate and protect themselves against cybersecurity attacks in smart factories	Can identify known attack patterns (e.g. the WannaCry and NotPetya malware)	Can detect all cybersecurity incidents in their smart factories	Leaders are able to discover abnormal behavior (such as machines working beyond defined parameters)

● Leaders   ● Others

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2020; N=950 organizations.

26

Smart & Secure? Why smart factories need to prioritize cybersecurity

03

Key challenges in bringing smart-factory cybersecurity up to speed

Organizations face challenges in onboarding partners and employees to their cybersecurity agendas

While organizations have recognized the increased incidence of cyberthreats and believe themselves to be aware of the risks involved, they need to ensure they onboard key stakeholders: employees and suppliers/partners.

Employee awareness of cyberthreats is inadequate

Our research shows that organizations face challenges in training employees to deal with various aspects of evolving cyberthreats. Not all organizations surveyed said their smart-factory employees are trained to deal with and mitigate the impact of cyberattacks made through connected machinery systems. As a first line of defense, employees must be made aware of the early-warning signs of a potential attack, ensuring a quick response.

Worryingly, not many of the organizations surveyed also claimed that their cybersecurity teams (employees / on-site contractors) have the required knowledge and skills to carry out urgent security patching without external support. One common cause for this widespread inadequacy is the lack of a cybersecurity leader in the business to spearhead the required upskilling program. This, when coupled with the scarcity of cybersecurity talent for smart factories, becomes a significant challenge: 57% of organizations say that the scarcity of smart factory cybersecurity talent is much more acute than that of IT cybersecurity talent.

As a Senior Director of Infrastructure and Security at a large consumer product group puts it: *"I don't think there is a lack of willingness to learn, there is just a lack of champions."*

Mansi Thapar, former Head of Information Security, CISO, at Jaquar Group, an Indian bathware and sanitaryware manufacturer, adds: *"Now, a lot of spending will be seen on automation training. Everything now will be IT- or IIOT-enabled, so they need to have some basic level of security for the foreman or someone on the factory floor. We really need tech-savvy people who at least understand the security."* [11]

Challenges arising from vendors/partners

"Shadow IT" (the trend of functions other than the main IT department employing discrete IT systems to bypass the shortcomings of the central system) has become a key challenge for organizations in recent years, and the pandemic has only exacerbated the issue. Our research uncovers that 77% of organizations are concerned about the regular use of non-standard smart factory-specific processes to repair or update OT/IIOT systems. This challenge partly originates from the low availability of the correct tools and processes. A significant share of organizations (51%) said that smart-factory cyberthreats primarily originate from partner and vendor networks.

Another challenge is building an effective security system from the plethora of security tools available, with the risk of misconfiguration leaving organizations open to cyberattack. Mansi Thapar adds: *"The main challenge is: there are so many vendors, so, which one to select? I can take the best product on the market but, if it is not implemented properly, then it is a waste; moreover, misconfigurations are one of the key reasons why a breach happens."*[12]

Delay in discovery of cyberattacks can worsen losses

A cyberthreat that is discovered before it can fully execute its intended attack can mitigate potential losses. These losses range from the financial, arising from damages to reputation, to regulator-imposed fines in light of inadequate preparedness. Our survey reveals that this is a major challenge for organizations. Many organizations surveyed say delay in discovery of cyberattacks has led to more severe losses for them. Extended time to recovery is a close second reason for higher losses.

Lack of collaboration between cybersecurity teams and the C-suite

Smart-factory cybersecurity is often evaluated at plant or regional level and does not receive the global board-level priority accorded other functions in the organization. Our research shows that there is a disconnect between the perceptions of C-suites and those of smart-factory leaders: more than half of respondents say that smart-factory leaders need to collaborate more closely with the Chief Security Officer(CSO) of their organizations.

Additionally, as smart factories proliferate, training cybersecurity experts who can oversee the implementation of comprehensive Industry 4.0 security measures will be essential. Our research shows that IT and OT cybersecurity currently suffers from a skills gap in this respect. Almost half of respondents say that their smart-factory cybersecurity team does not communicate adequately with the enterprise IT team. The lack of communication hinders efficient deployment of cybersecurity preparedness and response, potentially overwhelming and delaying discovery and response to a cyberthreat.

Shomayle Ahmad Faruqi, Cyber Security Architect at Otis, a US elevator and escalator manufacturer, explains the potential pitfalls: *"There are organizations trying to train IT people to work in an OT environment and OT people to work for the IT department, so that IT and OT work hand in hand. But there was a lot of conflict between them, because the person working in the OT department for two decades had a very different perception of OT than the person [who had been] working in IT."*

Lack of budget bites

A comprehensive budget that caters to the unique requirements of each plant and site is essential to ensuring efficient use of resources. Around 53% of respondents say that cybersecurity budgets for smart factories are still allocated from the local/site budget. The lack of dedicated budgets also leads to the possibility of funds being diverted to other areas of smart factories that appear to need immediate attention.

A dedicated budget ensures that the long-term goal of achieving smart-factory cybersecurity is not compromised. This is another challenge commonly faced by respondents to our survey. More than half say that smart-factory cybersecurity budgets are factored into the cost of product manufacturing. Such organizations also run the risk of being unable to secure budgetary approval for these initiatives. Shomayle Ahmad Faruqi of Otis Elevator adds: *"Usually, OT is sidetracked, and it is made like a support department; hence, budget allocation is impacted"*

77%

of organizations are concerned about the regular use of non-standard smart factory-specific processes to repair or update OT/IIOT systems
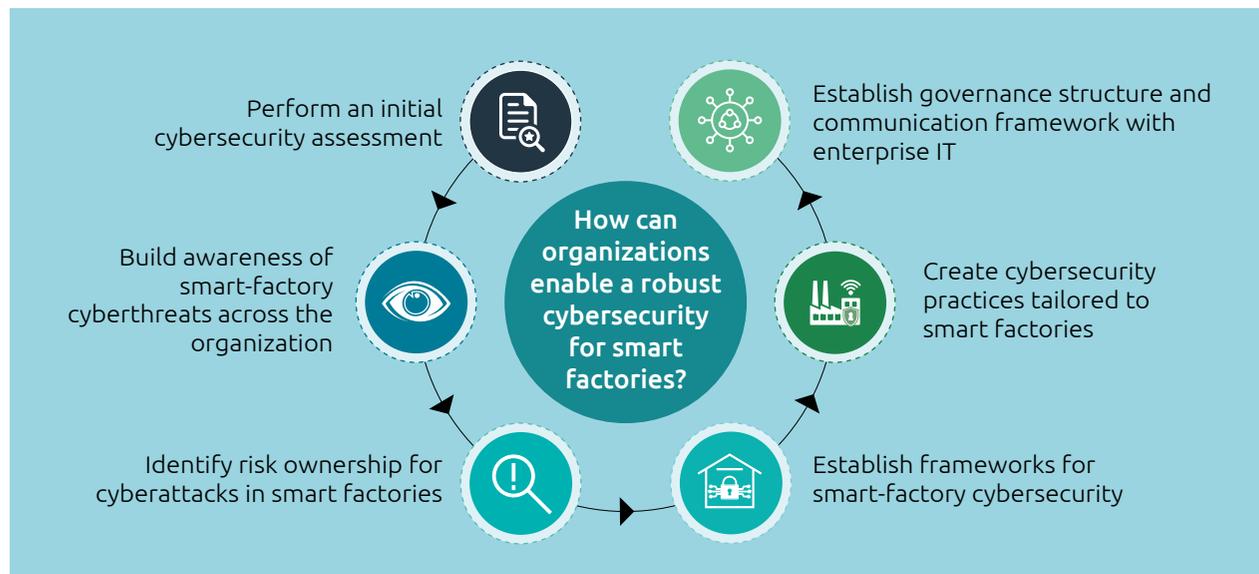
04

How can organizations implement robust cybersecurity in smart factories?

Fig.7

A framework for cybersecurity in smart factories

We segregated the organizations in our survey sample into two segments: Cybersecurity Leaders and the rest. We analyzed the practices of Cybersecurity Leaders and found they were distinguished from other organizations across multiple dimensions. We define Leaders as those organizations that have mature practices across three critical pillars of cybersecurity: awareness, preparedness, and implementation of cybersecurity in smart factories. (Please refer to insert "Cybersecurity Leaders take the market advantage" for more details.) Based on our analysis and insights from industry leaders, we recommend the following actions for organizations to enable implementation of robust cybersecurity in smart factories:

Perform an initial cybersecurity assessment

Establish governance structure and communication framework with enterprise IT

Build awareness of smart-factory cyberthreats across the organization

How can organizations enable a robust cybersecurity for smart factories?

Create cybersecurity practices tailored to smart factories

Identify risk ownership for cyberattacks in smart factories

Establish frameworks for smart-factory cybersecurity

Source: Capgemini Research Institute Analysis.

Perform an initial cybersecurity assessment

A risk analysis based on specific attack scenarios for factories allows organizations to identify and evaluate risks and to decide which to accept and which they need to mitigate. This risk assessment can then be used to build a tailored cybersecurity system across all smart factories and identify the maturity of cyber-preparedness within the business as a whole. Shomayle Ahmad Faruqi at Otis Elevator elaborates: *"There is a very straightforward strategy for overcoming OT challenges and that is to carry out proper threat modelling and risk assessment for a separate OT environment."*

The first step is to create an inventory and tracking mechanism for all connected devices in the smart factory, in order to understand and assess the attack surface area. A total of 93% of Leaders have an inventory and tracking mechanism for all IIOT and unmanaged devices that are connected to the smart factory, compared to just 50% of other firms. This must be followed up by regular device-risk assessments, as conducted by 83% of Leaders, compared to 46% of others. These device-risk assessments help organizations to identify the vulnerable machinery that needs to be fixed. They also help organizations detect anomalous behaviors. For instance, 85% of Leaders are able to detect employees using

personal devices to connect with the machines at their smart factories, compared to just 49% of others.

Organizations need to build up a functional, systemic knowledge of their smart factories in order to establish a clear vision of where key vulnerabilities exist and where measures can be taken in different blocks such as the plant control tower, intelligent automation, mobility, and edge platforms. Overall, the share of network-connected devices that are tracked and monitored by cybersecurity tools in the smart factory must also be assessed and prepared to defend against attacks.

Apart from this heightened understanding of the operations-related aspects of the factory, it is also imperative that organizations understand the smart factory network interconnection pattern. This allows a more effective response to attack because it will be possible to identify immediately which function is impacted and adapt the remedial action to this systemic context. As many as 48% of organizations say there is a lack of cybersecurity talent well versed in smart factory manufacturing operations, leading to a failure in this aspect of preparedness.
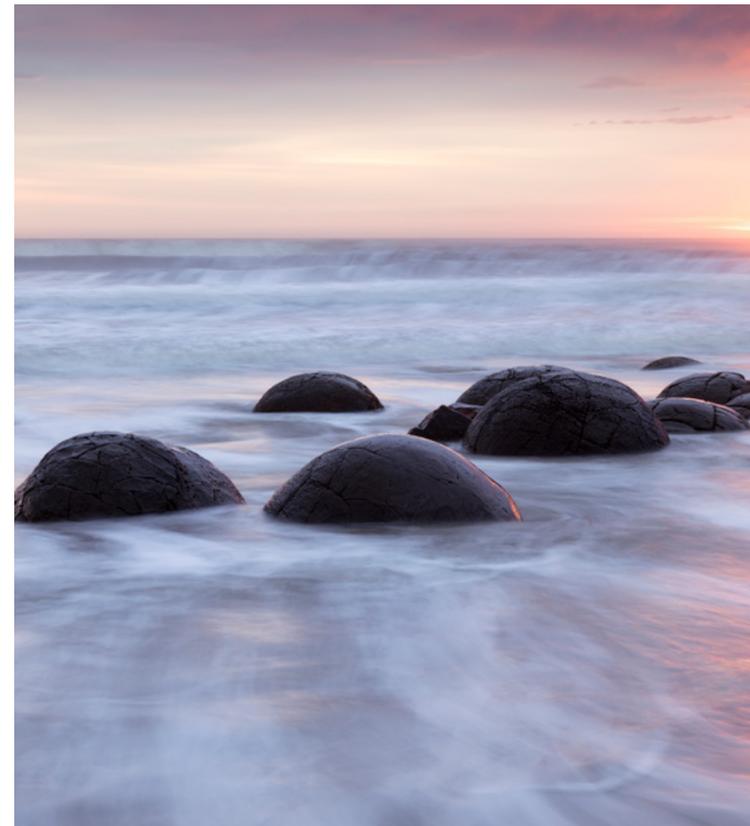
Build awareness of smart-factory cyberthreats across the organization

A significant 81% of Leaders say their smart factory employees are trained to deal with the impact of cyberattacks through connected machinery, compared to 46% of others.

It is vital that organizational management develop an awareness of the seriousness of the current lack of preparedness for cyberattacks, so that they prioritize the cybersecurity of smart factories. To emphasize the significance of this, 94% of Leaders run regular in-house training and cybersecurity-awareness programs for executive leadership, compared to 52% of others.

Given their stronger training infrastructure, Leaders are in a much better position in terms of preparedness than are non-Leaders: 81% of Leaders say their cybersecurity team (employees/on-site contractors) possess the relevant knowledge and skills to carry out urgent security patching independently and effectively without external support, compared to 48% of others.

The Head of Cyber Security Service Operation Center at a large European defense firm underlines this point: *"Awareness is very important at every level: for top management, to help let them make strategic investments, but also for employees, who are usually the weak links in the chain. Awareness and training should be spread to all the resources inside the company."*

Identify risk ownership for cyberattacks in smart factories

53%

of respondents say that cybersecurity budgets for smart factories are still allocated from the local/site budget.

85%

of Leaders say they have clearly defined lines of risk ownership for smart-factory cybersecurity, compared to 45% of the rest.

Around 53% of respondents say that cybersecurity budgets for smart factories are still allocated from the local/site budget. This can lead to smart-factory cybersecurity being sidelined. It is important for organizations to define risk ownership for smart-factory cybersecurity early on, as the business impact of cyberattacks on smart factories is typically high. C-suite executives must be alert to how the budget for smart factory cybersecurity is apportioned.

A senior executive in Industrial Control Systems at a global consumer product group adds: *"For any good risk assessment in OT, first we see that there should be proper IT-OT segmentation."* This is important: no potential attacker should be granted access to the organization's IT network via its OT system. The reverse is also important, as many cyber events have started with an IT breach and then traversed to OT.

Unplanned downtime of just four hours can cost a manufacturer as much as $2 million.[13] Identifying risk ownership prior to a cyberattack is critical; 85% of Leaders say they have clearly defined lines of risk ownership for smart-factory cybersecurity, compared to 45% of the rest. The risks should be further analyzed to identify non-standard processes; 89% of Leaders have a system for recognizing unmanaged risks and non-standard processes and systems.

Risk assessment can help an organization make the best use of available resources – both financial and human.

Organizations must also develop a detailed, robust roadmap that sets out the varying risk structures. Progressive steps that incorporate various business stakes, risk profiles, and priorities can help organizations implement cybersecurity solutions without impacting the architecture of the production line.

Establish frameworks for smart-factory cybersecurity

A governance mechanism that adheres to globally accepted cybersecurity protocols for smart factories and is aligned with the wider supplier and vendor ecosystem is essential. As many as 93% of Leaders (compared to 43% of others) have an OT/IIOT security-governance program that adheres to international cybersecurity protocols and regulations, such as those set by the International Electrotechnical Commission (IEC), the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and The National Cybersecurity Agency of France (ANSSI).

Governance protocols also help to ensure global rollout of patches and threat updates; 98% of Leaders update their OT/IIOT threats based on a global protocol for all smart factories, compared to 48% of others. Moreover, 81% of Leaders also build and update OT/IIOT current-state cyber assessments and report back to leadership, compared to 43% of others. To enable this, cybersecurity must be engrained in the very design of a smart factory. Our research found that, for many organizations, cybersecurity is not a major design factor; only 51% build in cybersecurity by default in their smart factories.

Tailor cybersecurity practices to the smart-factory environment

Adopting integrated, enterprise-wide cybersecurity is self-evidently beneficial, but can nevertheless prove seriously problematic if not implemented properly. Serge Maillet, Country Segment Manager – Industrial Networks and Cyber Security at Siemens, an industrial automation company, confirms: *"The convergence can bring in tremendous benefit to organizations, especially in terms of increasing business and operational efficiencies, while also reducing costs – an increasingly important factor. However, it does come with its own set of challenges. Inadequate cybersecurity measures and controls with IT and OT convergence will only compound this problem and increase the attack surface."*[14]

Given this scenario, organizations are looking to build specialist cybersecurity teams specifically for smart factories: 89% of Cybersecurity Leaders have a cybersecurity team focused specifically on OT/IIOT threats to smart factories, compared to just 51% of others. Also, 89% of Cybersecurity Leaders have a security operations center (SOC) that can provide a real-time, 360-degree view of all connected devices and IIOT assets, identifying threats or unusual IIOT traffic, compared to 47% of others.

However, only 65% of Cybersecurity Leaders have a dedicated SOC for smart-factory cybersecurity and enterprise IT. Nevertheless, this is still far ahead of the 36% among others. It is also important that organizations maintain an up-to-date "cybercrisis playbook" to ensure that smart factory operations teams know which protocols to follow in the event of an attack.

Given the absence of a robust cybersecurity framework in the majority of smart factories, developing and nurturing cybersecurity talent within organizations is critical. Given the scarcity of talent, automation will be essential going forward. For instance, the effort to maintain manually updated security certificates for each known asset in smart factories is challenging. Automating the frequency and updating of the certificates will be vital to helping the cybersecurity talent focus on threat mitigation and response. Moreover, prototyping the cybersecurity solution in a pilot program allows implementation teams to develop an in-depth understanding of that solution, such as whether the installation process will be straightforward and patchable with the proposed automation framework. Such preparation will ease the implementation process proper, enabling faster deployment and minimizing production impact.

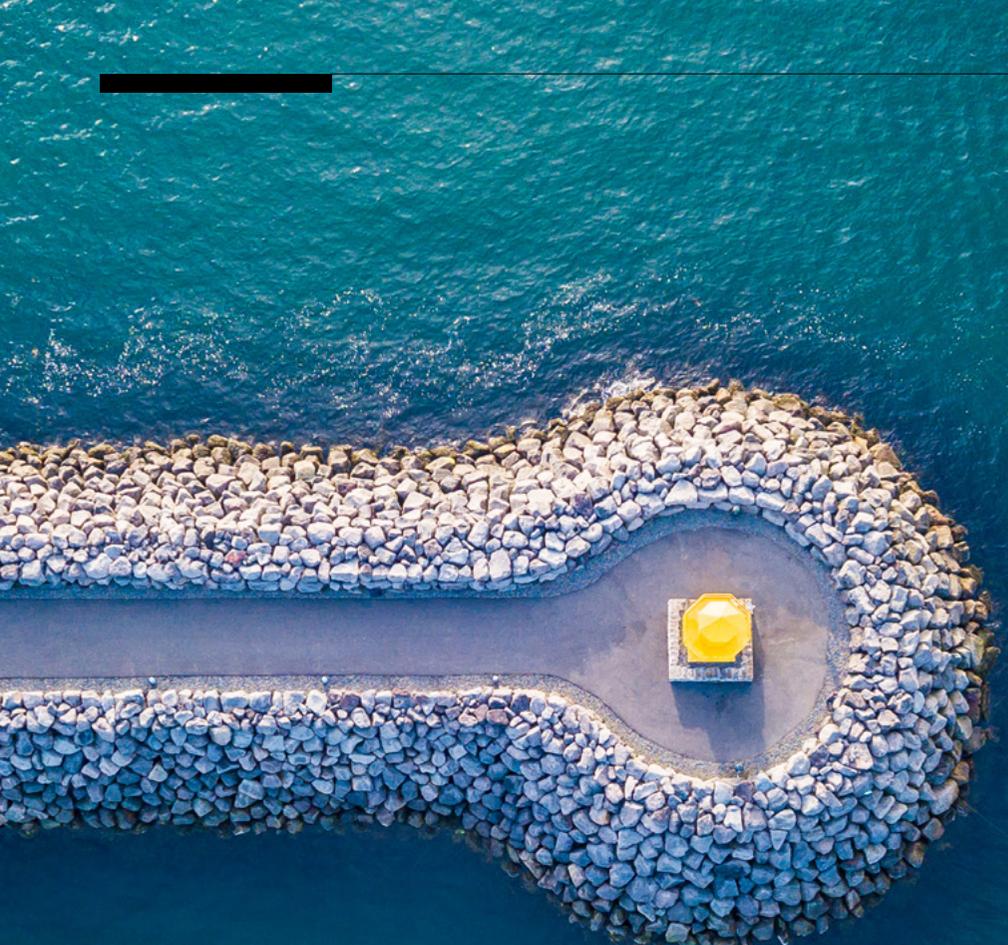# Establish a governance structure and communication framework with enterprise IT

Smart-factory cybersecurity governance should be conducted through a matrix structure that affords local decision-making autonomy to the smart-factory cybersecurity team, with a dotted line reporting to the CISO. This ensures that the on-site cybersecurity team collaborates well with the plant managers and provides the CISO with visibility of the organizational cybersecurity strategy.

We found that 70% of Leaders' smart-factory cybersecurity teams regularly communicate with enterprise IT cybersecurity teams to plug gaps in security requirements, compared with 48% of others.

The key to effective cybersecurity is to have teams that know and understand the functioning of the production chain and the industrial equipment and networks, in order to be able to analyze events in detail and, above all, build a remedial plan to minimize the production impact. To achieve this, a cybersecurity representative from the operational teams should be embedded within the factory; this should be an individual who already possesses a very good knowledge of the factory, who can help analyze alerts and, above all, contribute to the construction of the remediation plan.

 The Global CISO at an international personal-hygiene group agrees: *"Group cybersecurity is steered by the CISO, where we set the strategy that provides goals and objectives. My direct reports include cluster managers responsible for a subset of countries. In each smart factory, we have cybersecurity teams who collaborate with the plant manager but ultimately report to cluster managers. This way, each plant focuses on how to align their security with the defined standards, goals, and technology."*

+ Conclusion

Smart factories are undoubtedly the way forward for manufacturing. However, it is important that organizations acknowledge that the increased attack surface area and greater harnessing of IIOT devices render them viable targets for hackers, potentially jeopardizing business interests. Organizations across the world are aware that this is, and will continue to be, an area of concern for manufacturers, and that they must raise their levels of preparedness for this threat.

There are multiple challenges that organizations face in implementing cybersecurity in smart factories, from low prioritization on the part of C-suite executives, to smart-factory cybersecurity being delegated to manufacturing-site leaders. Organizations that implement cybersecurity measures effectively are able to respond and mitigate threats. It is as simple as that: in the Industry 4.0 era, organizations must adapt to survive in the cyberspace where most business now takes place.

Research Methodology

Fig.8

Organizations by country

To understand how organizations are securing their smart factories and the challenges they must overcome to do so, we surveyed 950 organizations globally in October and November 2021.

We also conducted one-on-one interviews with a range of senior cybersecurity officers across sectors.

*The study findings reflect the views of the people who responded to our online questionnaire for this research and are aimed at providing directional guidance. Please refer to the methodology for details of respondents and get in touch with a Capgemini expert to understand specific implications.

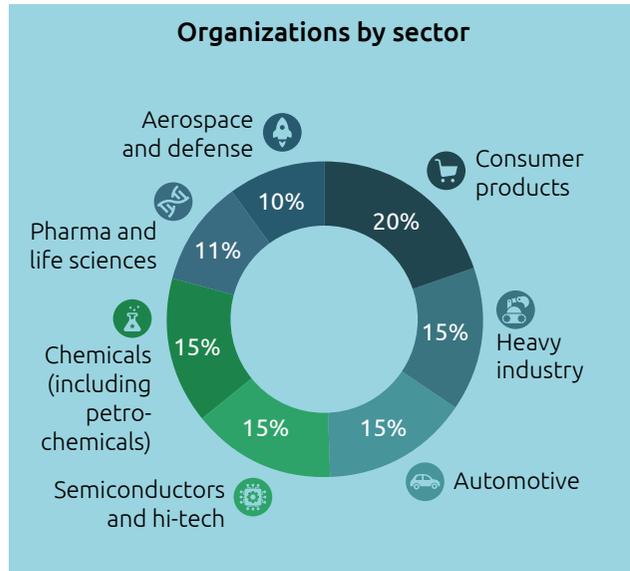**Organizations by country**

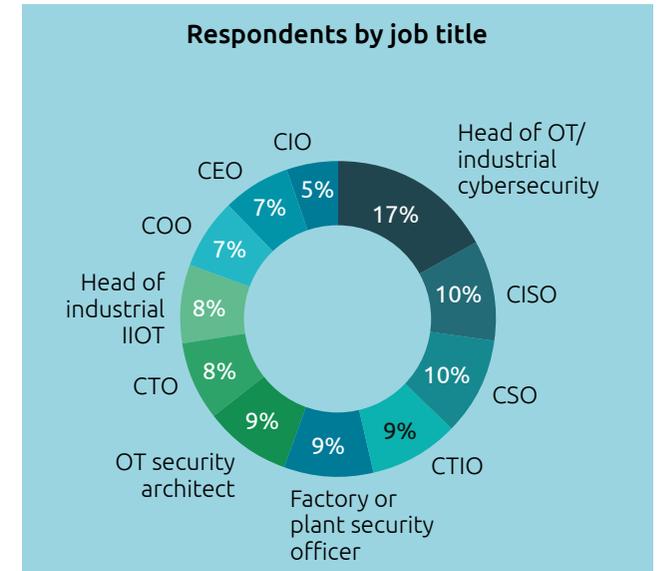| Country	
Australia	11%
Italy	11%
UK	11%
US	11%
France	11%
Germany	11%
Spain	10%
Nordics	10%
India	6%
China	5%
Netherlands	5%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.
Numbers may not total 100% owing to rounding.

Organizations by sector

Aerospace and defense 10%
Consumer products 20%
Pharma and life sciences 11%
Heavy industry 15%
Chemicals (including petro-chemicals) 15%
Automotive 15%
Semiconductors and hi-tech 15%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Organizations by revenue

More than US$50b 13%
US$500m - 999m 18%
US$20b - 49.99b 13%
US$1b - 4.99b 17%
US$10b - 19.99b 17%
US$5b - 9.99b 22%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Respondents by job title

CIO 5%
CEO 7%
Head of OT/ industrial cybersecurity 17%
COO 7%
Head of industrial IIOT 8%
CISO 10%
CTO 8%
CSO 10%
OT security architect 9%
CTIO 9%
Factory or plant security officer 9%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

+ Appendix

Below are the questions used to gauge the cybersecurity preparedness of the organizations for our research. (Figure 6)

On a scale of 1–5, how would you rate your organization's preparedness on the following parameters:

Protection	Score
Rate the level of preparedness on the following scale: 5 – Very high level of preparation 4 – High level of preparation 3 – Medium level of preparation 2 – Low level of preparation 1 – Very low level of preparation	
a. Level 0 – Production Process Control (e.g., sensors, actuators, meters)	...
b. Level 1 – Basic control (sensing and manipulating; e.g., PLC)	...
c. Level 2 – Monitoring and supervising (e.g., HMI, SCADA)	...
d. Level 3 – Manufacturing operations management (e.g., MES)	...
e. Level 4 – Business planning and logistics control (e.g., ERP)	...

Governance	Score
Rate the statements on the following scale: 5 - Strongly agree 4 - Agree 3 - Neutral 2 - Disagree 1 - Strongly disagree	
a. Cybersecurity in the smart factory is a C-Level concern for manufacturers.	...
b. We have a senior leader who can bridge IT and OT/IIOT priorities and mandates.	...
c. The OT/IIOT and IT cybersecurity systems are connected in our organization.	...
d. Our leaders want to invest in smart-factory (OT/IIOT) cybersecurity as the current manufacturing process is working well.	...
e. Level of implementation of cybersecurity governance in plants.	...
f. We have an OT/IIOT security-governance program adhering to international cybersecurity protocols and regulations (e.g., IEC, CIS, NIST, ANSSI).	...

Detection & Resilience	Score
Rate the statement on the following scale: 5 - More than 80% 4 - 60%-80% 3 - 40%-60% 2 - 20%-40% 1 - Less than 20%	
a. Share of network-connected devices that are tracked and monitored by cybersecurity tools in your smart factory.	…
Rate the statements with the following scale: 5 - Strongly agree 4 - Agree 3 - Neutral 2 - Disagree 1 - Strongly disagree	…
b. We can detect cybersecurity incidents in our smart factories.	…

	Score
c. We can identify known attack patterns (e.g., WannaCry, NotPetya)	…
Rate the statements on the following scale: 5 - Strongly agree 4 - Agree 3 - Neutral 2 - Disagree 1 - Strongly disagree	Score
d. We have a team dedicated to cyberattack response and recovery at smart factories.	…
e. We have an incident-response mechanism for all OT/IIOT cybersecurity threats.	…
f. We have a cybersecurity team focused specifically on OT/IIOT threats to smart factories.	…
g. Our employees at smart factories are trained on the impact of cyber-attacks through our connected machines.	…

Appendix

⊘ **Awareness**	**Score**
Rate the statements with the following scale: 5 - Strongly agree 4 - Agree 3 - Neutral 2 - Disagree 1 - Strongly disagree	
a. We update OT/IIOT threat intelligence periodically.	...
b. We update our OT/IIOT threats based on a global protocol for all our smart factories.	...
Rate the level of preparedness on the following scale: 5 – Very high level of preparation 4 – High level of preparation 3 – Medium level of preparation 2 – Low level of preparation 1 – Very low level of preparation	...
c. Plant control tower – e.g., remote monitoring, IIOT track, and trace, etc.	...
d. Intelligent automation – robots/cobots, additive manufacturing, etc.	...

e. Real-time information management – PLC, MES/ SCADA, IIOT.	...
f. Quality analytics and adaptive testing – plant analytics and AI.	...
g. Energy management – smart energy management.	...
h. Plant maintenance – analytics and AI, predictive analytics, etc.	...
i. Enhanced operator – enhanced worker skills with AR/VR, remote assistance, etc.	...
j. Mobility and Edge platforms.	...

The level of preparedness across your organization.

Score	Level of preparedness
Greater than 120	Very high level of preparation
90-120	High level of preparation
60-90	Medium level of preparation
30-60	Low level of preparation
Less than 30	Very low level of preparation

Appendix

+Reference

1. Verdict, "Industrial IoT connections expected to reach 37bn by 2025," November 2020.

2. Capgemini Research Institute, smart factories survey, April–May 2019; N=1,348 manufacturers.

3. WSJ, "Unilever focuses on factory cybersecurity as pandemic sparks run on consumer staples," December 2020.

4. AHL, "Mike Towers' collaborative approach to information security," March 2019.

5. Capgemini Research Institute, smart factories survey, April–May 2019; N=1,348 manufacturers.

6. The Manufacturer, "Half of Britain's manufacturers have been the victim of cyber-security attacks in last 12 months," May 2021.

7. Verdict, "Industrial IoT connections expected to reach 37bn by 2025," November 2020.

8. Manufacturing Global, "Cybersecurity: making manufacturing secure," May 2020

9. Financial Express, "Continental receives TISAX certification for cybersecurity in R&D and manufacturing," January 2022.

10. PRN News, "SecurityGate.io selected by Chevron to help them scale global OT cybersecurity," September 2020.

11. CIOL, "Panel discussion on OT Cybersecurity for manufacturing," September 2020.

12. CIOL, "Panel discussion on OT Cybersecurity for manufacturing," September 2020.

13. IIOT World, "The actual cost of downtime in the manufacturing industry," November 2018.

14. CIO, "Bringing IT and OT together is a critical Industry 4.0 challenge," November 2021.

+Authors

Geert Van der Linden
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

Didier Appell
Head of OT/IIoT cybersecurity
didier.appell@capgemini.com

Aarthi Krishna
Global Head of Intelligent Industry Security
aarthi.krishna@capgemini.com

Pierre-Luc Refalo
Vice President, Head of Group Cyber Risk Management
pierre-luc.refalo@capgemini.com

Jerome Buvat
Global Head
Capgemini Research Institute
jerome.buvat@capgemini.com

Subrahmanyam Kanakadandi
Senior Director,
Capgemini Research Institute
subrahmanyam.kvj@capgemini.com

Sumit Cherian
Senior Manager,
Capgemini Research Institute
sumit.cherian@capgemini.com

Yashwardhan Khemka
Manager, Capgemini Research Institute
yashwardhan.khemka@capgemini.com

Darshil Shah
Associate Consultant,
Capgemini Research Institute
darshil.shah@capgemini.com

About the Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on the impact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom, and the United States. It was recently ranked number one in the world for the quality of its research by independent analysts.

Visit us at www.capgemini.com/researchinstitute/

+ For more information, please contact:

Global contact

Geert van der Linden
Practice Head, Cybersecurity & CISO GBL-CIS
Head Global Cybersecurity Practice Hub
geert.vander.linden@capgemini.com

Joe McMann
Global Head of Portfolio, Cybersecurity Services
joe.mcmann@capgemini.com

Jerome DESBONNET
Chief Technology Officer, Cybersecurity Services
jerome.desbonnet@capgemini.com

Aarthi Krishna
Global Head of Intelligent Industry Security
aarthi.krishna@capgemini.com

Didier APPELL
Head of OT/IoT Cybersecurity
didier.appell@capgemini.com

Regional Contact

APAC
Samir Khare
samir.khare@capgemini.com

Australia
Keith Betts
keith.betts@capgemini.com

United Kingdom
Julie Clark
julie.clark@capgemini.com

Netherlands
Dennis de Gues
dennis.de.geus@capgemini.com

North America
Dave Cronin
dave.cronin@capgemini.com

Brazil
Leonardo Silva Carissimi
leonardo.carissimi@capgemini.com

France
Nolwenn LE STER
nolwenn.le-ster@capgemini.com

Italy
Giorgio La Spina
giorgio.laspina@capgemini.com

Nordics
Anders Askåsen
anders.askasen@capgemini.com

Southeast Asia
Hamsa Siddique
hamza.siddique@capgemini.com

+ Secure IoT/OT Services

Securing your critical IoT/OT infrastructure

Capgemini's Secure IoT/OT services bridge the siloes of legacy IoT/OT security, bringing together everything needed to see, understand, and mitigate the risks in your environment. Capgemini provides services to improve the IoT/OT security posture of your whole installation (Networks, Machines, Endpoints, devices, PLC, Applications, etc.). Our approach is to reuse proven solutions in IT and adapt them to the industrial context:

- **Availability and Integrity** before confidentiality
- **Security consistent with Safety**
- **Operational use cases driven** (operations constraints and production shutdown risks)
- **Maintain system performance** (despite real-time constraints, old technologies)

In short, we converge OT/IT/IoT/IIoT security so you can focus on **mitigating the risk of production losses** while exploiting digital transformation and Industry 4.0 business opportunities—rather than worrying about the next breach.

Why partner with capgemini?

Many companies claim to have IoT/OT security expertise. What is truly unique about Capgemini's experience and capabilities in this arena? Here are just a few examples:

OT expertise: Capgemini has many years of experience securing enterprises with critical OT processes and infrastructure, and provides a holistic end-to-end service (Assess, Protect, Check, Maintain, and Monitor).

Deep, sector-specific cybersecurity experience:

Capgemini has the breadth and depth of skills to cover security requirements in virtually every industry and market segment, including natural resources, energy and utilities, manufacturing, healthcare and life sciences, automotive, telecommunications, and more—with negligible operational impact and zero downtime.

Business-first approach: Our expertise is not limited to security technology. We see the big picture from a business perspective and can help you implement IoT/OT security that advances your digital transformation and Industry 4.0 goals.

Strong partnerships: We work with the "Who's Who" of IoT-related security partners, and their offerings complement and add value to our Secure IoT/OT Services. Our partners include Claroty, Fortinet, IBM, Microsoft, Nozomi, Otorio, TrendMicro, Zentera, and many more.

Global scale: Capgemini is everywhere your development teams, networks, devices, and users are with nearshore delivery capabilities worldwide and our integration expertise enables you to scale on demand whenever, wherever you want.

Satisfied clients: Our clients are achieving tremendous business value and are highly satisfied with the services they receive. We encourage you to ask us for references in your industry sector

Take the next step toward secure enterprise IoT/OT

Let Capgemini help you implement digital transformation and Industry 4.0 initiatives with confidence. Contact us today. Let's discuss your business objectives and explore how our Secure IoT/OT Services can advance your strategic priorities.

Visit our website to know more about Secure IoT/OT Services:
https://www.capgemini.com/service/cybersecurity-services/enterprise-iot-security/

Follow us on LinkedIn:
https://www.linkedin.com/showcase/intelligent-cybersecurity/

✚ Discover more about our research

The data-powered enterprise: Why organizations must strengthen their data mastery

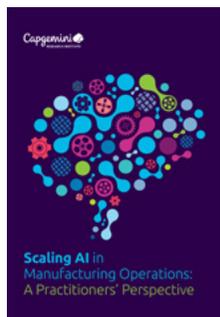**Conversations for tomorrow Intelligent Industry: The Next Era of Transformation**

Accelerating the 5G industrial Revolution

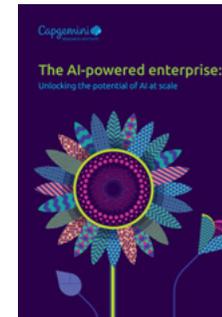**Sustainable operations A comprehensive guide for manufacturers**

How automotive organizations can maximize the smart factory potential

Scaling AI in Manufacturing Operations: A Practitioners' Perspective

Smart Factories @ Scale

The AI-powered enterprise: Unlocking the potential of AI at scale

Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security

+ Subscribe to latest research from Capgemini Research Institute

Receive copies of our reports by scanning the QR code or visiting

https://www.capgemini.com/capgemini-research-institute-subscription/

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 340,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | **www.capgemini.com**