

AXA XL Insurance

Operational Resilience

Managing cyber risk when digital systems meet physical processes

Produced in partnership with: DENEXUS | Deloitte.

XL Insurance

To learn more about exclusive cybersecurity services from AXA XL, please activate your CyberRiskConnect access.

1. Click here to **Request Access** or use the **QR code** and enter your contact details.
2. In the following days, you should receive an email with a link to create your password and set up your account. Please use it soon as the link will expire in 5 days.
3. Once you've set the password for your account, you can then use this link to login **CyberRiskConnect**.
4. In case of technical issues with the login, any requests, or feedback you may have, please reach out to our Client Excellence team at: **dcp_customer_support@axaxl.com**
5. Clients in the US or Canada who would like to access CyberRiskConnect should contact Gwenn Cujdik at: **gwenn.cujdik@axaxl.com**

DENEXUS

www.denexus.ai

About DeNexus

DeNexus and DeRISK are trademarks of DeNexus, Inc.

DeNexus™ is building the global standard of industrial cyber risk quantification for boards, shareholders, investors, capital markets and the risk transfer market. The DeRISK™ Intelligence Platform puts OT cyber-physical risk in financial terms, so industrial operators, insurers and investors can quantify, reduce and transfer it. DeNexus has supported 300+ DeRISK CRQ v5 implementations across the US and EU. AXA XL is a strategic investor in DeNexus. Headquartered in Boston, with an office in London.

Please note AXA Digital Platform is a private site for customers of AXA XL only. Do not share portal access instructions with anyone outside your organization. You are responsible for maintaining the confidentiality of the access code provided to you. Up to five individuals from your organization may register and use the portal. This portal contains a directory of experienced providers of cyber risk management and breach services. Services are subject to the terms and conditions between the Vendors and customer. AXA XL is not responsible under any circumstances for the services provided to customers by Vendors. Before you engage any of these companies, we urge you to conduct your own due diligence to ensure the companies and their services meet your needs. Unless otherwise indicated or approved, payment for services provided by these companies is your responsibility. Services may not be available in all regions and in local languages.

Contents

Foreword 4

Executive summary 5

When cyber risk meets the physical world 6

A more connected operational environment 7

Why securing OT requires a different approach 9

Threat, disruption and financial consequence 11

Operational risk is moving up the agenda 12

Crossing the cyber-physical line changes the loss equation 13

Building a clearer view of OT risk 15

How cyber disruption can stop a physical process 16

Containing the spread of disruption 17

Preparing for decisions under pressure 18

Moving towards a more intelligent operational landscape 19

The AXA XL approach 20

Final reflections 21

Disclaimer 22

Foreword

Operational Technology (OT) rarely receives the same attention as IT, yet much of modern life depends on it. It controls the systems that keeps clean water flowing, power moving across grids, transport running safely and essential manufacturing operating – the systems that are crucial to the businesses and services we rely on every day.

Historically, OT has often operated in relative isolation, managed by specialist teams and designed first and foremost around safety, reliability and performance. That has made it less visible than enterprise IT. The shift towards more connected OT environments began more than a decade ago, as businesses sought to improve performance, anticipate faults, and make better use of operational data. Since then, connectivity has become increasingly embedded in how physical operations are managed. These systems run on information that's constantly moving between physical equipment, corporate systems, cloud platforms and external suppliers. It is a flow of information that creates value for businesses and the people who rely on their services, but also makes physical operations dependent on a wider footprint of technology, networks and providers.

That wider dependency and exposure gives cyber attackers more opportunities. Interfering with a supporting IT system, compromising supplier access or creating doubt about the integrity of equipment can be enough to halt an operation, even if the attacker never reaches machinery or devices themselves. And the consequences of a cyberattack can extend far beyond the loss of data. Production and essential services may stop, expensive finished goods or materials may be wasted, equipment can be damaged, and in the most serious cases, people or the environment may be placed at risk.

For the engineers, technicians and field operators responsible for these environments, the priority remains keeping physical processes safe, reliable and productive. Cyber risk management must support that responsibility by identifying where interconnection creates exposure, how an incident could affect the process, and what actions would maintain or restore operations safely.

For operations, risk and business leaders, the challenge is to translate these scenarios into operational and financial consequences, identify the processes they cannot afford to lose, and direct investment towards the measures that reduce risk most effectively.

At AXA XL, we believe this resilience planning is central to achieving stronger cyber readiness. This report, which includes expert insights from DeNexus and Deloitte, explores the changing OT landscape, and outlines the practical steps businesses can take today to achieve long-term resilience.



Jonathan Salter
Head of Risk Consulting

Executive summary

Operational Technology (OT) supports the physical processes behind industries ranging from manufacturing, transport, energy and water to logistics, healthcare, and commercial buildings. As these environments become more connected, the cyber risk surrounding them is becoming more consequential. An incident can interrupt production, restrict access to essential systems, damage equipment, or create safety and environmental risks.

Five developments in particular should shape business leaders' priorities:



Cyber risks are becoming physical

An incident does not need to directly compromise machinery to interrupt operations. The loss, compromise or suspected compromise of connected IT systems can itself be enough to halt production or restrict the systems needed to operate a site safely.



Connectivity is extending the path to disruption

Operational environments increasingly depend on cloud platforms, enterprise applications, remote access, shared identity services, virtualization infrastructure, external suppliers, and connections between sites. These links support more efficient and responsive operations, but also create additional routes through which disruption can reach critical processes.



OT changes the cyber risk calculation

OT equipment tends to have long lifecycles, strict safety requirements, and limited maintenance windows. Security controls designed for enterprise IT cannot simply be applied in the same way. Protection must account for the operating tolerances, availability requirements, and physical consequences of the environment itself.



The consequences can extend far beyond cyber

Cyber incidents might begin with stolen data or an extortion demand, but financial impact can grow rapidly once physical operations are affected. Lost output, waste materials, missed customer commitments and supply-chain disruption can follow, with the most severe events creating the potential for injury or environmental harm.



OT makes resilience particularly dependent on operational context

Asset visibility and recovery planning matter across cybersecurity generally, but they become especially important in OT because interventions themselves can affect production and safety. Leaders need to know which systems are vulnerable, and what they control, what depends on them, and how the physical process could be operated or restored safely during or after a cyber incident.

Key Learning

Businesses need to understand what their OT controls, the critical systems, connections and suppliers it depends on, and how operations could be maintained or restored safely.

When cyber risk meets the physical world

OT works quietly behind much of daily life. Cyber incidents affecting it can begin in several ways. Some start in corporate IT and spread into connected operational environments; others exploit supplier or remote-access routes; and a smaller number directly target industrial control systems. Whatever the route, the potential consequences increase significantly once technology capable of influencing a physical process becomes involved.

Safety and availability have traditionally dominated decisions about OT, often leaving cybersecurity at the margins. And even where the risk is recognized, common security measures may be difficult to apply. For example, an update that is routine on an office laptop may require extensive testing and a carefully planned maintenance window before it can be applied to equipment running a continuous or safety-critical process.

For senior leaders, OT security has to begin with the physical industrial process. Organizations need to identify where digital systems monitor, manage or control physical equipment and processes, what would happen if those systems failed or operators lost visibility, and which decisions could safely be taken if they became unavailable or could no longer be trusted.



A more connected operational environment

Greater connectivity has transformed the role of OT. Systems once designed to perform a defined task within a single site now produce real-time information that businesses use to optimize performance and maximize asset output, while enabling operations to be monitored and supported remotely.

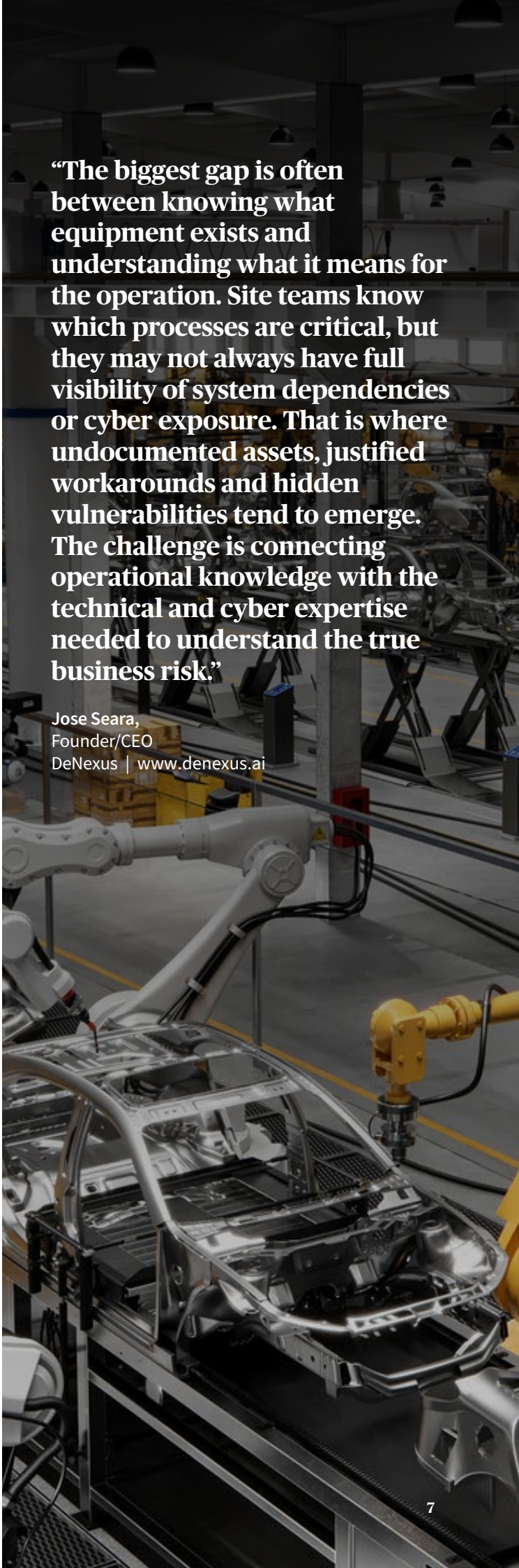
Take a manufacturing production line as an example. Connected sensors and control systems can monitor machinery, temperature, pressure and production output in real time, helping operators identify potential faults earlier, optimize performance and reduce unplanned downtime. But these systems may also exchange data with corporate applications, cloud platforms and specialist suppliers, creating dependencies that extend beyond the production environment itself.

This greater exchange of data delivers clear operational benefits, but it also means services outside the OT environment can become essential to keeping physical operations running. Recent warnings show how directly this exposure can translate into disruption. In August 2026, the UK National Cyber Security Centre[1] warned of increased targeting of OT systems across multiple sectors globally, specifically highlighting risks created by internet-exposed systems, legacy connections, and unmanaged assets.

The consequences are already visible. In July 2026, the FBI reported cyber incidents affecting water and wastewater organizations[2] across at least seven US states after malicious actors accessed internet-facing programmable logic controllers. Some incidents degraded water operations, including loss of pressure and flooding.

Some organizations assume their OT is protected because it is 'air-gapped', meaning it is physically separated from corporate networks and the internet. But wireless links, removable media, undocumented or informal supplier access – including connections established for remote

1 UK National Cyber Security Centre, Disruptive cyber activity highlights risk from internet-exposed systems and edge devices, 2026
2 Federal Bureau of Investigation, Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions, 2026



"The biggest gap is often between knowing what equipment exists and understanding what it means for the operation. Site teams know which processes are critical, but they may not always have full visibility of system dependencies or cyber exposure. That is where undocumented assets, justified workarounds and hidden vulnerabilities tend to emerge. The challenge is connecting operational knowledge with the technical and cyber expertise needed to understand the true business risk."

Jose Seara,
Founder/CEO
DeNexus | www.denexus.ai

maintenance – and legacy connections can still create routes into an apparently isolated environment. When these exceptions accumulate without central oversight, they can produce a web of connectivity and exposure that no single team fully understands. Without a clear view of these connections, organizations cannot properly assess or manage the exposure they create.

Connected operations improve efficiency and control. The objective is not to reverse that progress, but to understand and manage each material connection, why it exists, who can use it, what depends on it, and what could happen if it were compromised, unavailable or could no longer be trusted.

Key Learning

Connected OT needs deliberate oversight. Organizations should understand the external systems, remote-access routes and suppliers supporting critical processes, removing or tightly controlling connections that are not necessary.



Case Study

When IT disruption affects physical operations

A cyber incident disrupted critical IT systems used by a major manufacturer, leading it to pause production across multiple sites. Operations were restored gradually following an extended period of downtime, with the effects also felt by organizations within its supply chain.

The incident did not need to directly compromise machinery or industrial control systems to affect physical operations. Production depended on connected IT systems, meaning disruption to the wider digital environment was enough to bring manufacturing to a halt.

The example demonstrates how IT disruption can translate into operational consequences as physical processes become increasingly dependent on interconnected technology.

Key Learning

An OT incident does not have to begin in OT. Businesses should identify the IT systems and services their physical operations depend on, then test what would happen if they became unavailable[1] or could no longer be trusted. This can expose dependencies capable of stopping production even when operational equipment itself remains unaffected.

1 Australian Cyber Security Centre, Guidance for Australian critical infrastructure

Why securing OT requires a different approach

Many cybersecurity frameworks, controls, and working practices have developed around enterprise IT and data security, where systems can be updated or temporarily taken offline with manageable disruption. Those same approaches become more complicated when technology controls physical outcomes, whether that's keeping a production line moving, regulating water quality, or maintaining safe conditions inside a reactor.

Industrial equipment often remains in service for decades, long after its operating system or communications protocol becomes obsolete. Replacing it may require specialist procurement or a planned shutdown, while even routine patching can interrupt production or take several days to reverse if something goes wrong.

Security testing can carry operational risks of its own. An aggressive network scan may place an unexpected load on an aging controller that automatically directs a piece of equipment or process. A configuration change could affect the timing of a sensitive process, such as regulating the chemicals used to treat water or the inputs in a pharmaceutical batch. Understanding the operating tolerances of any equipment is therefore essential before applying controls that appear straightforward elsewhere.

The visibility and scale of that equipment is another persistent challenge. Large businesses often operate thousands of devices across factories, warehouses, commercial buildings and remote sites, with some installed many years ago, while others are maintained by suppliers and may not appear in businesses' central inventory.



"Businesses should start with the outcome a control is meant to achieve, then find the safest way to deliver it in that environment. Where a control cannot be applied directly, a compensating control elsewhere in the system can provide equivalent protection. For example, if a workstation or server can only be patched during an annual shutdown, application allow listing or virtual patching can reduce exposure until then."

Mohamed Kameche
Partner
Deloitte

The visibility challenge is significant. In a 2025 SANS survey[3] of industrial cyber professionals, only 12% of respondents had full visibility of how an attack could progress from an initial IT compromise to the controllers and physical processes deeper within OT. Without understanding what each asset supports, how it is connected and what recovery would require, teams cannot reliably prioritize the areas of greatest business risk. A little-known engineering workstation, for example, may be critical if it is used to configure equipment across several sites.

Only 12%

of respondents had full visibility of how an attack could progress.
- 2025 SANS survey

Responsibility for OT risk is often spread across different parts of organizations too. Engineers might understand the machinery and safety implications; IT and security teams might manage networks, identities and cyber threats; suppliers might control maintenance access or hold specialist knowledge.

These responsibilities vary significantly from business to business and are often unique to each organization, meaning they need to be mapped properly. Bringing them together allows an organization to assess how cyber weaknesses could affect safety, continuity and financial performance, and to agree which exposures are the biggest priority.

That clarity is equally important when an incident occurs. Security teams may push to disconnect equipment, while operations leaders might contest that an abrupt shutdown could waste expensive finished goods or materials, damage machinery or complicate recovery. Preparedness should establish how these decisions will be made and who has the authority to make a final decision, before the business is placed under pressure.

The controls chosen need to reflect equipment lifecycles and the practical reality of keeping physical operations running. Operational context is crucial to make sure risk assessments, security investment, and response planning are effective.

3 SANS ICS/OT Cybersecurity Survey, 2025

Key Learning

Security controls must reflect the safety, equipment and continuity requirements of each operational environment, with clear ownership of the risks that could cause the greatest harm.



Threat, disruption and financial consequence

For attackers seeking to pressure a business, few things create urgency like the prospect of operations coming to a standstill. Every hour lost carries a cost, and leaders may have to act before they fully understand what has been compromised. The consequences can become even more serious when an incident compromises the safety and protection systems designed to protect people, equipment or the environment.

This makes OT-dependent businesses attractive targets for ransomware groups, even when attackers have little intention or ability to manipulate industrial equipment directly. The convergence of IT and OT technologies in the last 40 years has made disruption easier and potentially more effective. Industrial cybersecurity company Dragos[4] tracked 119 ransomware groups affecting more than 3,300 industrial organizations in 2025, an almost 50% increase in active groups from the previous year. Its incident response team observed significant operational disruption in every OT ransomware case it handled during the year.

An attacker does not necessarily need control of machinery to disrupt operations. Encrypting corporate systems, stealing privileged credentials or disrupting applications used to schedule, monitor, or support production may be enough. If operators cannot confirm that equipment is functioning safely, uncertainty alone can justify a shutdown. Similarly, if certification data needed to confirm product quality for food or regulatory compliance is unavailable, finished goods may no longer be able to be sold.

Greater connectivity can increase that threat. Remote maintenance and supplier access allow internal engineers and external suppliers to diagnose faults, install updates and support equipment without being on site. While the operational benefits are clear, the access needed for this work can shorten the distance

4 Dragos OT/ICS Cybersecurity Report, 2026



"OT scenarios are different because the potential consequences extend beyond data or system availability. An attack may indirectly disrupt operations, deliberately target OT using relatively crude methods, or use sophisticated OT-specific techniques to manipulate control, suppress alarms or disable safety functions. As that targeting becomes more specialised, the potential consequences increase too, from outages and damaged equipment to environmental harm, fire, injury or other serious cyber-physical impacts."

Donovan Tindill,
OT Cyber Senior Director
DeNexus | www.denexus.ai

between enterprise IT and critical operations, making it easier for bad actors to escalate attacks once they have found a way in. One compromise at a trusted supplier may provide a route into several sites or businesses, while poorly secured remote access or stolen credentials can allow attackers to move at pace through connections that were created to support day-to-day operations.

The threat is not only limited to financially motivated groups. Critical infrastructure and strategically important industrial businesses make very attractive targets for state-backed actors seeking longer-term access, or the ability to cause disruption during periods of geopolitical tension. In such cases, their aim can be less about immediate financial gain, and more about mapping out operational environments, to create more damaging disruption to essential services in future.

As IT and OT become more interconnected, compromising the systems, identities and providers that operations depend upon can be enough to create uncertainty and force difficult decisions.

Operational risk is moving up the agenda

The potential for cyber incidents to disrupt physical operations is changing expectations of organizational accountability. OT risk increasingly crosses the boundaries between engineering, security, operations, enterprise risk, and senior leadership.

Regulation is reinforcing that shift. In the European Union, for example, the NIS2 Directive5 strengthens requirements around cyber risk management, incident reporting and management accountability for organizations operating in critical sectors, while the Cyber Resilience Act (CRA)[6] sets mandatory cybersecurity rules and introduces incident reporting obligations. For boards and executive teams, OT cyber risk increasingly needs to be understood as part of operational resilience and business continuity, rather than as a specialism sitting solely within engineering or security teams.

Key Learning

Boards should have clear oversight of material OT cyber exposure, supported by defined operational ownership and plans covering the systems, identities and suppliers on which critical operations depend.

"Ownership should ultimately sit with the executive accountable for operational performance, typically the chief operating officer or the asset owner, because they bear the consequences when production stops. Conflicts tend to arise when each group keeps its own risk register and speaks its own language. A shared OT risk taxonomy, a single governance forum with genuine decision-making authority and named individuals accountable to that forum remove most of the ambiguity."

Mohamed Kameche
Partner
Deloitte

5 EU NIS2 Directive, European Commission
6 EU Cyber Resilience Act, European Commission

Crossing the cyber-physical line changes the loss equation

The financial impact of a cyberattack can widen rapidly as disruption moves from business systems to physical operations. An incident may begin with stolen data or an extortion demand, but if production then stops, the costs of lost output, missed deliveries and contractual penalties can quickly outweigh the initial cyber-response costs or extortion demand.

The route from compromise to loss is rarely clean or predictable. An attacker may leave industrial equipment untouched, yet production still stops because operators have lost access to scheduling or monitoring systems. Elsewhere a compromised account may allow direct interference with a controller.

For many, interruption is the largest and most immediate risk. Revenue can quickly fall while wages and emergency costs continue, materials may be lost, and delays can spread quickly through tightly sequenced supply chains.

"Two sites using similar technology can still face very different financial exposure. The scale of loss depends on factors such as production capacity, revenue, the nature of the physical process and what is being handled. Pressure, toxicity, combustion, movement, nearby populations or sensitive environments can all multiply the impact of an incident, as can the cost of business interruption, clean-up, regulatory action and liability following physical damage or harm."

Jose Seara,
Founder/CEO
DeNexus | www.denexus.ai



Case Study

When uncertainty stops operations

A major industrial services company experienced significant business disruption following a ransomware attack that affected parts of its corporate network. Although critical operational systems were not directly compromised, several activities were temporarily restricted while the organization investigated the incident and assessed potential impacts. Operations were gradually restored over the following days, resulting in service delays and the activation of contingency measures.

Key Learning

Uncertainty about whether an incident has reached OT can be enough to stop a critical operation. Response plans should clearly define when systems or equipment must be isolated based on identified criteria. They should specify what teams need to confirm before restarting, including that the incident has been contained, equipment settings have been checked, and operations can resume safely.

Restoring services can take much longer than removing malware. Teams may need to validate controller logic, inspect equipment and restart machinery in a safe sequence, with one in five respondents saying full remediation takes more than a month, according to a 2025 SANS institute survey.[7] Such extended recovery times create an accumulation of costs that can span production, contractors, customers, and the wider supply chain.

1 in 5

respondents say that full remediation takes more than a month.
- SANS Institute Survey, 2025

In the most severe cases, an attacker can manipulate the physical process itself and cause changes to speed, pressure, temperature, or chemical composition of products, all of which may affect equipment quality and efficacy, or create unsafe conditions. Environmental harm and injury are relatively infrequent, but their potential severity changes the risk calculation significantly.

Remember here that businesses often use the same machinery, software, or suppliers across several locations. So, a weakness in one widely deployed product has potential to interrupt multiple facilities.

7 SANS ICS/OT Cybersecurity Survey, 2025

Dependencies shared across an industry can create the co-exposure potential for one compromised provider to affect numerous businesses at once.

These different pathways matter when considering insurance. Costs may touch cyber, property, business interruption, equipment breakdown, environmental, casualty or liability policies, depending on the circumstances and the terms of cover. For example, a shutdown taken as a precaution may present different questions to the physical damage caused by malicious manipulation.

This complexity reinforces how important it is to map credible scenarios as part of any risk management exercise – and crucially, before any incident. Doing so helps businesses identify where protection exists, which exposures may require more mitigation, and how they can best insure themselves against future risk.

Key Learning

The cost of an OT incident is shaped by the physical process, the decisions made under pressure, and the time required to recover safely. Scenario planning should follow the full path from initial compromise to operational interruption, physical consequences, and wider supply chain loss.



Building a clearer view of OT risk

Managing OT risk starts with identifying which physical processes matter most to the business, and what they depend on. A complete inventory of equipment is part of that picture, but a list of devices alone cannot show where disruption could cause the greatest harm.

The process has to start with assessing the operation itself. Which production lines, utilities, safety functions or building systems are critical? How long could each be unavailable before the consequences become serious? How long can they continue to operate in isolation from other networks or systems (e.g., disconnected from IT or Internet access)? What would be needed to operate safely by hand, move production elsewhere, or safely restore the process?

Having answers to these questions brings operational, financial and cyber risk into the conversation, and provides a platform for a more informed and judicious process. It helps businesses to direct time and investment towards weaknesses that could cause the greatest disruption, even when they are not rated as the most technically severe.

This is an important exercise, given most critical processes now rely on more than the equipment visible at a site. They may depend on an enterprise identity service, a cloud platform, a central control system, specialist software, or remote support from a supplier. Power, GPS, telecommunications and other utilities add further dependencies outside the organization's direct control.

Mapping these dependencies helps expose routes through which disruption could spread and reveals single points of failure, such as one workstation operating systems across several plants or a supplier whose credentials provide access to multiple operational environments.

Building this operational picture requires care. Techniques used routinely to discover devices on enterprise IT networks can interfere with sensitive or ageing equipment. Information may therefore need to come from passive monitoring, engineering records, site inspections, and conversations with those who operate and maintain processes.

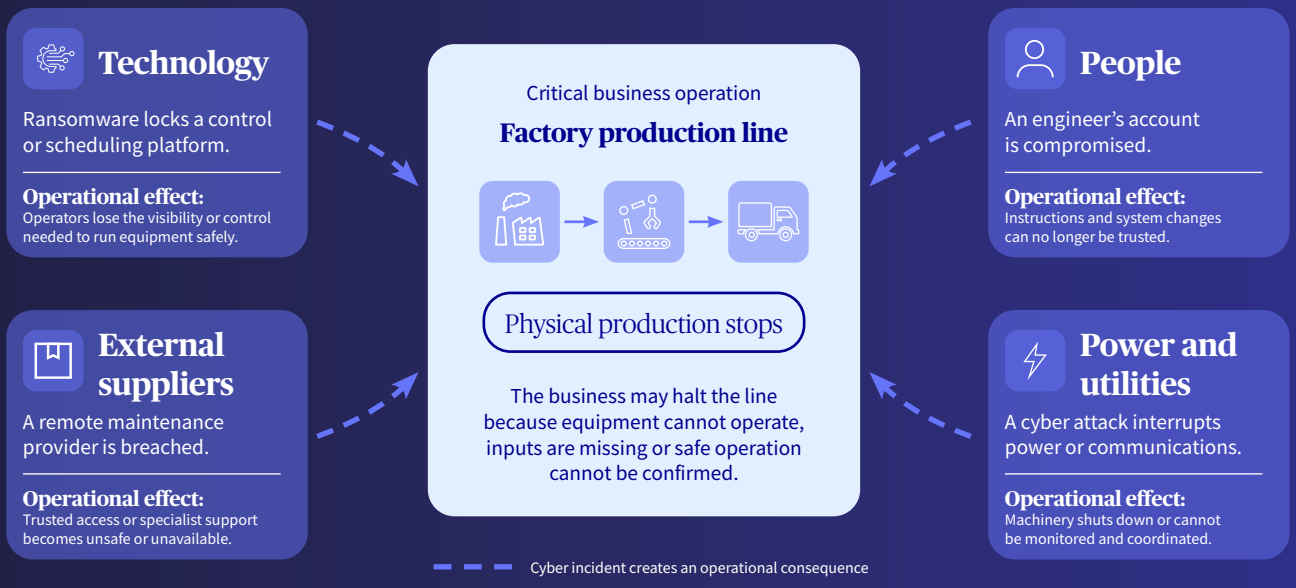


"Programs rarely stall at the assessment stage, but rather just afterward. Vulnerabilities are identified, but remediation has no clear owner, is funded year by year, and ends up competing with production priorities. The organizations that sustain progress translate findings into operational objectives, adopt an operating model that reflects how decisions are really made, whether at headquarters or site level, and commit to funding remediation over several years."

Mohamed Kameche
Partner
Deloitte

How cyber disruption can stop a physical process

A production line relies on technology, people and services beyond the machinery itself. Disruption to any critical dependency can leave the business unable to operate safely.



"OT cyber risk needs to be quantified differently from conventional IT risk. Financial impact can extend beyond data breach or extortion to include prolonged operational interruption, damaged equipment and materials, health and safety impacts, environmental consequences and OT-specific liabilities. Putting financial values against those scenarios gives organizations a much stronger basis for prioritizing investment, particularly where legacy technology cannot be quickly patched or replaced and mitigation choices need to be justified."

Donovan Tindill,
OT Cyber Senior Director
DeNexus

Key Learning

Build an inventory that shows what each critical asset supports, what it depends on, who can access it, and what would be required to restore it safely. This creates a practical basis for risk-based decisions, rather than another administrative exercise.

Containing the spread of disruption

With that understanding of critical routes and dependencies established, businesses can focus on limiting how far disruption can travel. IT and OT networks should be appropriately segregated, with controlled interfaces between them. Effective segmentation limits the pathways available to an attacker, helping prevent a compromise in corporate systems from moving freely towards critical machinery or from one operational site to another.

Those boundaries need to reflect how operations genuinely work. Controls that prevent engineers from carrying out essential tasks, for instance, risk being bypassed by employees. Similarly, undocumented or temporary connections can quietly undermine otherwise sound technical or security architectures.

Remote and third-party access deserves particular attention. Permissions should be limited to the systems and periods required for the work, protected with strong authentication and withdrawn when no longer needed. Activity should be monitored wherever possible so that unusual behavior can be identified and events can be reconstructed before, during and after an incident.

It's worth noting that legacy equipment may not support these protections directly. In such cases, network isolation can protect it indirectly by placing it in a separate zone and limiting which systems are allowed to communicate with it. Monitoring these connections can help to identify unexpected activity and reduce exposure while replacement is planned around investment cycles and operational shutdowns.



"External access should be treated as an operational process: designed, approved and monitored like any other. Organizations need a live view of who is connecting, what they can reach and why. Supplier access should pass through a single managed gateway, with multi-factor authentication, least-privilege, just-in-time permissions, and session recording. Contracts should set these requirements from the start. Done well, this makes legitimate support faster rather than slower."

Mohamed Kameche
Partner, Deloitte

Key Learning

Segmentation should be treated as a baseline OT security requirement. Connections between enterprise IT, operational networks and third parties should be deliberate, controlled and monitored so that compromising one system or account cannot provide unrestricted access to critical operations.

Preparing for decisions under pressure

OT incident planning must account for the physical consequences of intervention. Disconnecting a system, closing a valve or stopping a production line may prevent further harm, but could also waste expensive finished goods or materials, or introduce risks to safety, equipment and product quality.

Although the impacts are physical, planning should start by assessing an organization's hierarchy, specifically, who has authority to isolate equipment and approve a restart. Cyber and operational teams need to understand who takes the lead when production needs stopping, including when decisions need to move to senior management.

Exercises should test technical response processes too. A ransomware scenario could explore how the business established whether OT had been affected, decide whether production could continue safely, and determine what evidence is required before operations restart. It could also test how the organization would communicate with customers, regulators, insurers, and other stakeholders while those decisions are being made.

Alongside those organizational assessments, recovery planning needs to extend to data integrity and architecture, not just everyday business data. Configuration files, controller logic, engineering documentation, software versions and access to specialist suppliers may all be necessary to restore a physical process safely. Their value depends on whether they are protected and capable of being used with equipment that remains available.

Following this process gives organizations the ability to measure risk in terms that leadership can act on: the proportion of critical processes mapped, high-risk connections removed, supplier access reviewed, recovery procedures tested, and priority weaknesses addressed.

That clearer view can support more meaningful conversations about risk transfer. Insurers and risk engineers can assess exposure more confidently when a business can explain how its critical operations are connected, what interruption could cost, how widely an incident might spread, and what recovery would require. The same work helps the business understand which losses it can reduce, which it may need to retain, and where insurance can provide a layer of financial protection.

Key Learning

OT incident plans should define who can isolate equipment, stop production and approve a safe restart. They should also include contingencies for prolonged disruption and be supported by exercises that test both the technical response and operational consequences.



Moving towards a more intelligent operational landscape

Operational environments are becoming more connected and more software-driven. Data that once remained within one site now flows into cloud services and shared platforms, while software plays a greater role in how equipment and processes are monitored, managed and adjusted. Everything from digital twins to autonomous machinery, edge computing and AI-enabled monitoring promises more efficient and responsive operations for organizations.

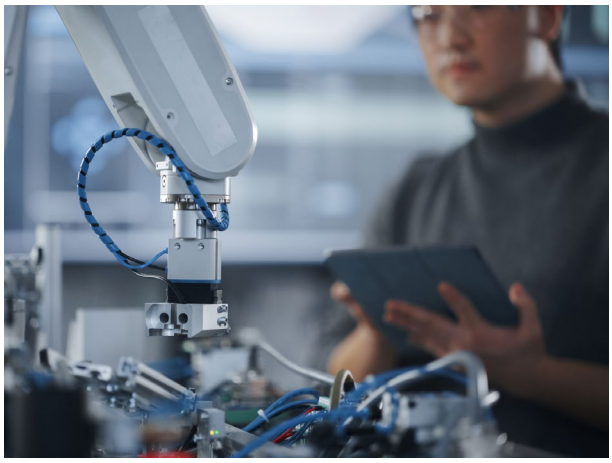
AI is already extending what businesses can learn from OT data. AI models can identify early signs of equipment failure and help operators adjust maintenance schedules before a fault interrupts operations. Over time, these systems may take on a greater role in optimizing energy use and supporting responses to operational incidents.

As that role grows, so does the importance of the information on which AI depends. Incomplete or manipulated data could give operators an inaccurate picture of what is happening on site. AI models can also become less accurate over time as equipment, materials, and operating conditions change. Consistently reliable outputs may also create overconfidence, and closer integration with AI may create common dependencies. If several facilities rely on the same model, cloud service or provider, one error or outage could affect multiple locations, while increased automation may erode the manual skills needed to run or restore a process.

Current international guidance[8] recommends that AI introduced into OT has a clear business case, is thoroughly tested, includes defined human oversight, and incorporates fail-safe mechanisms that protect the physical process.

Businesses making these investments today have a crucial opportunity to address these risks while systems are still being designed. New technology must be assessed against the process it will influence, the consequences if its output is wrong or unavailable, and operators' ability to safely challenge it or operate without it.

The choices made during this phase of adoption will shape operational exposure for years to come. Building visibility and recovery into new systems from the outset can prevent today's innovation from becoming tomorrow's legacy risk.



8 Australian Cyber Security Centre "Principles for the secure integration of AI in OT" guidance

Key Learning

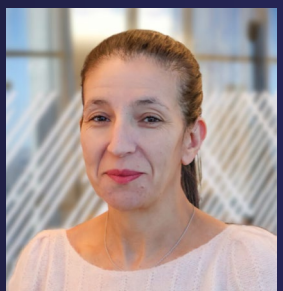
As AI takes a greater role in physical processes, organizations should test how systems behave when data is wrong, models fail, or external services become unavailable, while ensuring operators can challenge, override or continue without them.

The AXA XL approach

OT risks are specific, and in many cases unique, to the environment in which they exist. The potential consequences depend on what the technology controls, how critical operations are connected and the extent to which they rely on ageing equipment, external suppliers and shared systems. AXA XL's objective is to help clients translate that operational complexity into a clearer understanding of cyber exposure, business consequence, and the actions that can materially reduce risk.

Our approach starts with establishing the operational context, identifying the systems, people, and dependencies behind critical processes. This provides a clearer view of where cyber disruption could occur and where resilience efforts should be prioritized.

We then work with our clients to turn technical findings into credible business scenarios. These might examine how ransomware within the corporate network could interrupt manufacturing, how compromised supplier access could create a route towards critical equipment, or how failure of a shared technology provider could affect several locations. Assessing the operational and financial consequences of these scenarios helps businesses to prioritize mitigation according to the exposures that could cause them the greatest harm.



Rebiah Bardot-Girard
Head of Cyber Risk
Consulting Services

Our work is grounded in recognized OT security standards. We align our assessments with IEC 62443-3-2[9], which provides a structured basis for assessing cybersecurity risk within industrial automation and control systems. This gives clients a consistent way to understand the operational environment, identify credible threats and vulnerabilities, and evaluate risk and determine the appropriate treatment.

We help clients strengthen preparedness through crisis exercises, training and recovery planning shaped around the realities of their operational environment. Where equipment cannot be patched or replaced without affecting operations or safety, we focus on practical measures that reduce exposure.

An insurer's perspective also helps translate cyber-physical scenarios into potential loss. Understanding how an incident could develop from initial compromise into operational interruption, physical damage or liability provides a stronger basis for deciding which exposures to mitigate, which to retain and where risk transfer has a role.

We combine our cyber, risk-engineering and insurance capabilities with specialist expertise from partners including Deloitte and DeNexus, spanning cyber prevention, operational resilience and risk quantification.

Together, these capabilities allow AXA XL to connect technical OT risk with operational and financial consequence, helping clients decide what to protect first, how to prepare for disruption, and how the remaining risk should be managed.

9 ISA/IEC 62443-3-2

Final reflections

Operational technology will continue to evolve, with significant gains promised by greater connectivity, automation, and the growing use of AI. As these technologies become more deeply embedded in physical operations, the distinction between cyber risk and operational risk will continue to narrow.

For business leaders, resilience starts with understanding that connection. Knowing which processes are critical, the technology and third parties they depend on, and how disruption could translate into operational and financial loss provides a stronger basis for deciding where to invest, what to protect and how to prepare.

That preparation needs to extend beyond preventing an attack, too. Organizations need to be ready to make difficult decisions when disruption occurs. Clear ownership, tested recovery plans and collaboration across cyber, engineering, operations and risk functions can make those decisions faster and better informed.

The true measure of OT resilience is whether a business can protect its most critical operations, make sound decisions under pressure, and recover safely when disruption occurs.



XL Insurance

Disclaimer

This report is the result of analysis from a wide variety of sources including publicly available reports, insights and analysis, and proprietary analysis and insights by AXA XL, DeNexus and Deloitte, based on their internal data. A non-exhaustive list of publicly available sources is included in the report but does not constitute the sole source of insights that made this report possible.

The analysis presented in this report is based on information available at the time of writing. When future evolution is expressed, it does not constitute prediction of the evolution of trends and threats, but the expression of the possible future context in which organizations may have to operate.

Global Disclaimer

Global Asset Protection Services, LLC, XL Catlin Services SE and their affiliates ("AXA XL Risk Consulting") provide loss prevention and risk assessment reports and other risk consulting services, as requested. In this respect, our property loss prevention publications, services, and surveys do not address life safety or third party liability issues. This document shall not be construed as indicating the existence or availability under any policy of coverage for any particular type of loss or damage. The provision of any service does not imply that every possible hazard has been identified at a facility or that no other hazards exist. AXA XL Risk Consulting does not assume, and shall have no liability for the control, correction, continuation or modification of any existing conditions or operations. We specifically disclaim any warranty or representation that compliance with any advice or recommendation in any document or other communication will make a facility or operation safe or healthful, or put it in compliance with any standard, code, law, rule or regulation. Save where expressly agreed in writing, AXA XL Risk Consulting and its related and affiliated companies disclaim all liability for loss or damage suffered by any party arising out of or in connection with our services, including indirect or consequential loss or damage, howsoever arising. Any party who chooses to rely in any way on the contents of this document does so at their own risk.

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details. This summary does not constitute an offer, solicitation or advertisement in any jurisdiction, nor is it intended as a description of any products or services of AXA XL.

AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL

Insurance, AXA XL Reinsurance and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: AXA XL Insurance Company Americas, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and AXA XL Excess & Surplus Lines Insurance Company. In Canada, insurance coverages are underwritten by XL Specialty Insurance Company – Canadian Branch. In Bermuda, the insurance company is XL Bermuda Ltd. Coverages may also be underwritten by Lloyd's Syndicate #2003. Coverages underwritten by Lloyd's Syndicate #2003 are placed on behalf of the member of Syndicate #2003 by Catlin Canada Inc. Lloyd's ratings are independent of AXA Group. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions.

AXA, the AXA and XL logos are trademarks of AXA SA or its affiliates. © 2026. Information accurate as of November, 2026.

axaxl.com