



Digital Resilience and Enterprise Recovery

Is your business prepared for a major cyber incident?
Proactive measures for IT/OT cyber security

What's inside

- 1 Executive summary
Overview and key actions you can take to be more prepared
- 2 Cyber attack - Not a question of if, but when and how severe
The typical response to cyber incidents affecting OT and key steps to recovery
- 3 When preparedness failed: Examining real life case studies
Case studies of major real-life IT/OT cyber incidents
- 4 Insights from major OT cyber incidents
Lessons learnt from OT cyber incidents we've responded to
- 5 Be ready to boost your resilience and recoverability
Why the "prepare" stage is a critical part of the incident response lifecycle
- 6 Conclusion
Preparing for the future
- 7 How we can help
Preparedness and response activities



Imagine being woken in the middle of the night by a panicked call from your operations manager: production at one of your key sites has suddenly stopped. It's one of your busiest times of the year.

Despite IT, operations and engineers trying all the usual fixes, nothing is working.

You don't know if this issue is isolated or if it's affecting your entire business.

Your answer arrives quickly but with alarming news: calls, voicemails, and texts from neighbouring sites report their production systems are also affected.

The impact is more severe than you could have imagined, leaving you panicked and shocked.

What would you do in this situation? Are you aware of your responsibilities? What actions would you take?

If you find yourself uncertain or hesitant, it is imperative to prepare now, before you find yourself in such a vulnerable position.

Don't leave it to chance; ensure you have solutions before it's too late.

This whitepaper provides practical steps you can put in place today to better prepare your organisation for a cyber attack.

Executive summary

With the rise of digitalisation, cyber threats against industrial sectors are also increasing. These threats range from accidental introduction of malware by employees to ransomware attacks by criminals or state-sponsored threat actors aiming to cause significant damage.

Drawing on our extensive experience of cyber security and Operational Technology (OT), including our Industrial Control Systems (ICS) subject matter experts in assisting clients during critical times, we have developed key recommendations to enhance your business and site preparedness. This paper examines the impact of major cyber incidents exploring emotional and operational consequences. It presents case studies of effective response strategies, identifies recurring challenges in cyber recovery, and outlines best practices for organisational response to such incidents. It offers practical steps to learn from our experiences and fortify your defences.

The journey to Digital, Industry 4.0, Internet of Things (IoT), Cloud and Artificial Intelligence (AI) offers substantial business benefits but also increases vulnerability to cyber-attacks.

While organisations have traditionally focused on protection and detection controls, we advocate for a robust recovery strategy to ensure resilience and quick wins as broader cyber security improvements are implemented.

A proactive approach to developing and implementing robust defence strategies can help safeguard your operations from potential cyber threats and build a more resilient future for your organisation.

Deloitte can support this journey by leveraging our insights and offering support from our industry experts. Together, we can build a secure and resilient future for your organisation.



Executive summary

Enhance your organisation's preparedness by taking these key proactive planning and testing actions today:

Map your critical business processes to assets

Directly link your critical business processes to the IT and OT assets they are reliant upon. This reveals how disruptions to your assets can impact critical business operations, allowing you to prioritise security initiatives and develop a restoration sequence.



Review disaster recovery plans

Review site Disaster Recovery and Business Continuity Plans (DR/BCP) for clarity, practicality, and effectiveness in addressing operational and cyber outage scenarios. It is important that plans are updated regularly in the case of a real incident affecting the shopfloor. Include communication plans, workarounds, restoration sequences for OT, and delegation of responsibilities for any essential staff who may be unavailable during an incident.



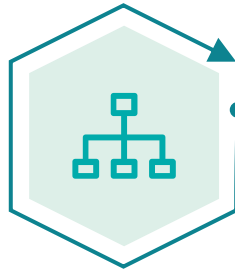
Ensure compromised vendors and/or supplier scenarios are considered

Cyber security criteria should be integrated into vendor selection, clear cyber security requirements should be established in contracts, and vendor security postures continuously monitored, leveraging threat intelligence.



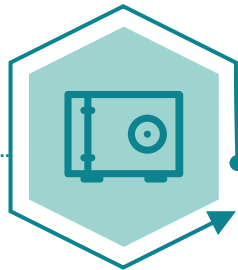
Prepare for network disconnection scenarios to maintain operations

Understand your site network architecture and know how you will disconnect your IT and OT during a cyber incident. Label these and make them easy to find. If the network infrastructure is affected, how does this affect production operations? Do you know the consequences of pulling the WAN cable?



Keep up-to-date, offline digital and physical backups of critical OT systems

To ensure operational continuity during cyber incidents, maintain offline backups of critical engineering files and system documentation, avoiding reliance on potentially compromised corporate networks. Additionally, leverage independently accessible cloud solutions for data redundancy and accessibility during outages.



Protect the most critical assets

During a cyber incident where IT services may be disrupted, malware may propagate to or from your OT network. Implement security controls and manage data flows to reduce the opportunity for malware to take hold or move. Protect critical assets by improving site architecture, following good practice, and implementing hardening recommendations.



Cyber attack - Not a question of if, but when and how severe

OVERVIEW

Cyber attacks pose a constant and evolving threat to operational environments. Senior leaders must be prepared to defend against these attacks and understand their responsibilities in mitigating the impact. The increasing volume and intensity of attacks mean organisations face daily ramifications, ranging from minor disruptions to significant financial losses.

Any entity with a digital footprint is potentially vulnerable to cyber attack. Observations from major industrial cyber incidents reveal a concerning trend: personnel responsible for the operation and management of industrial IT and OT are not prepared for responding to a cyber attack. It is often assumed that IT departments will protect OT sites from attack which proves inaccurate in practice.

“31% of respondents reported 6+ intrusions, compared to only 11% last year. In particular, organisations with advanced maturity levels reported high intrusions for this cycle.”

Source: 2024 State of Operational Technology and Cybersecurity Report, Fortinet

CYBER ATTACKS CONTINUE TO RISE

Cyber attacks on industrial organisations are increasingly affecting production performance at sites both directly and indirectly.

Technology integration, business process dependencies and the ongoing convergence of IT and OT environments has removed the clean separation between the two, exposing OT environments in ways never seen before.

While cyber security awareness is increasing, with many organisations recognising cyber risks on their risk registers, OT security often takes a backseat. This creates a false sense of security, as IT/OT vulnerabilities can directly impact production and the entire value chain. To ensure business resilience, organisational

leaders must start to prioritise OT security alongside IT security, recognising their interconnectedness in today's digital landscape.

“Manufacturing is the #1 targeted industry, four years in a row, representing 40% of incidents.”

Source: 2025 IBM Security X-Force Threat Intelligence Index

NOT ALL CYBER INCIDENTS ARE CREATED EQUAL

We frequently encounter situations where our experience has revealed common challenges in cyber attack preparedness, prompting us to consider the following three key questions:



Why do so many sites not have response and recovery processes in place to mitigate a cyber attack?



Why is there still such a lack of basic security controls protecting the OT environment?



Why did the board think they were prepared for a significant cyber incident, when really, they weren't?

Cyber attack - Not a question of if, but when and how severe

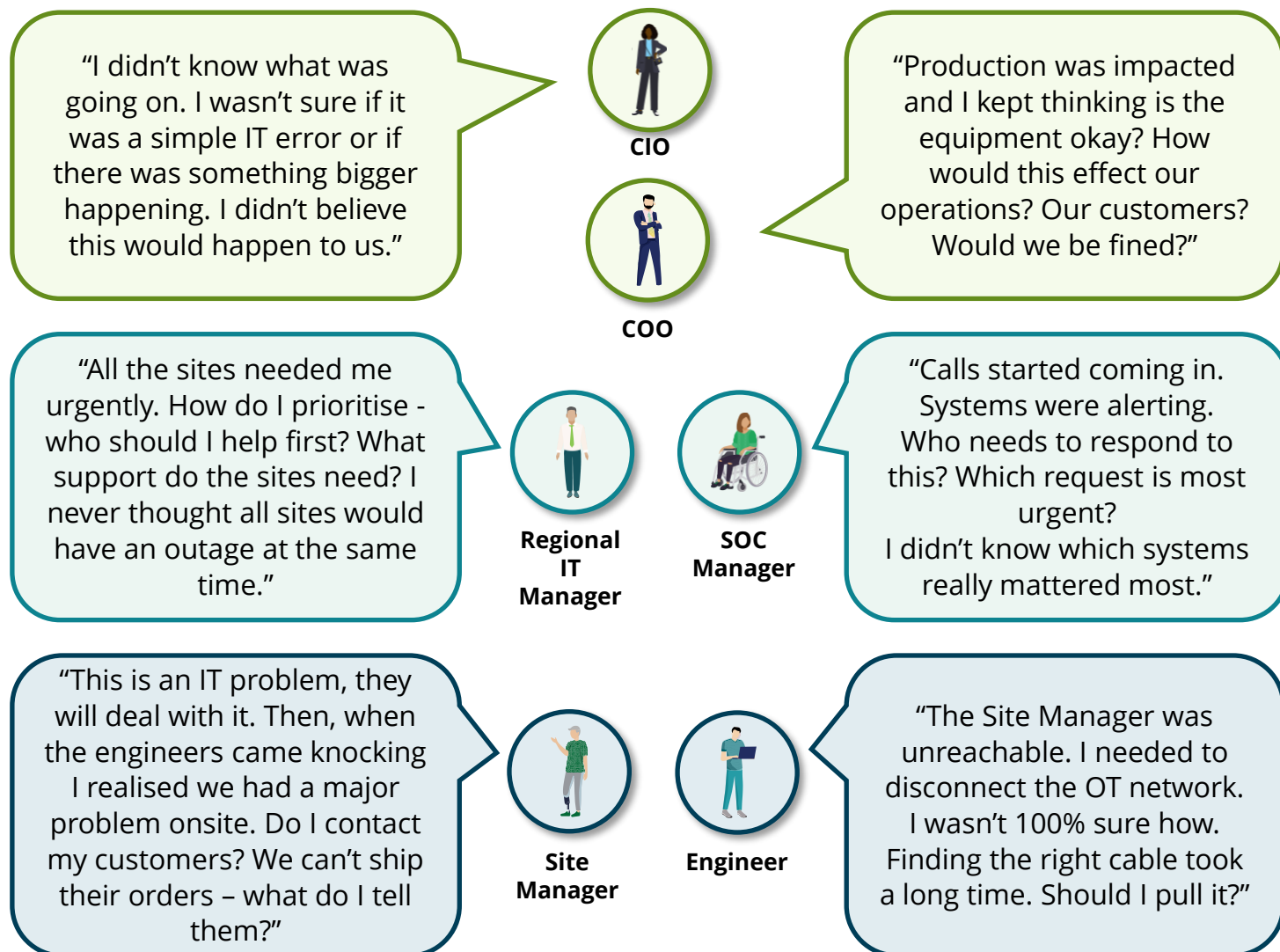
REALISING THAT YOUR OT IS AFFECTED

Systems aren't responding, screens are blank, others display rapidly changing data that doesn't reflect reality. Elsewhere operators are confronted with ransomware messages and are completely locked out of systems. Shopfloor technology connected to IT applications and infrastructure grinds to a halt, workarounds are rapidly identified and phones ring constantly.

Our clients, from engineers and operators on the shopfloor to CIOs in the boardroom have lived through all these moments. In these first few hours and days the immediate focus is on

the impact to business operations and the production environment. When things go wrong, making sure the site is safe and critical physical assets are protected is the priority.

The human response to significant cyber incidents often manifests as feelings of panic, chaos, and disorder. This can lead to uncoordinated and ineffective remediation efforts, particularly when individuals lack clarity on appropriate immediate actions.



Cyber attack - Not a question of if, but when and how severe

KEY STEPS IN RESPONSE AND RECOVERY

Unprepared organisations are forced to rapidly grasp the complex interplay of people, processes, and technology during a cyber incident. This often necessitates new collaborations and risk management approaches.

A lack of critical information during a cyber incident directly prolongs disruptions and their impact on business operations.

Facing major disruptions to their industrial IT and OT environments, organisations typically follow these common steps for response and recovery:

1

Disconnect OT from IT: The first step is typically to isolate OT systems as rapidly as possible and can be achieved in different ways. This raises the questions, who will authorise the disconnection of the OT network from the Enterprise, and when? And if the call is made, do people know where and how to execute this, central IT, site IT, engineers?

2

Maintain safety and control of shopfloor operations: Preserving the integrity and control of critical OT systems is important, either through containment or restoring the system as quickly as possible (once systems are confirmed as clean).

3

Keep production running: After core HSSEQ (health, safety, security, environment, and quality), business and site objectives shift to keeping operations running to maintain essential supply chain and customer dependencies. It often extends to moving product due to physical storage limitations when logistics systems are unavailable. Problems can be compounded due to the increasing use of IoT.

4

Move product or ship product to customers: The site may need to work with the wider business to move product. There may be reliance on and integration with enterprise resource planning, distribution, billing, staff payroll and manufacturing execution systems. The site may require resilient architecture or local workarounds to manage situations where critical IT is unavailable.

5

Enable site support services: Business recovery and remediation that restores normal business operations can only occur after critical enterprise IT and critical site operations have been returned to service.

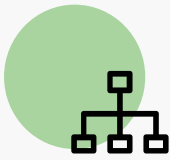
Cyber attack - Not a question of if, but when and how severe

OBSERVATIONS TAKEN FROM OTHERS

Every incident is unique, however, there are recurring themes:

Governance

Different management structures between IT, OT and business units affects the level and implementation of security controls across different sites, OT systems and devices.



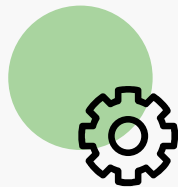
Information requirements

Locating critical information during a disruption can be extremely time-consuming, and sometimes even impossible.



Risk management

IT cyber risk is increasingly included within Enterprise Risk Management (ERM) while OT Cyber risk lacks adequate attention by the business and is rarely featured within existing risk management frameworks.



Physical damage

A cyber incident affecting OT systems can cause physical impacts to site equipment e.g. a silo outage stopping feed into an operational furnace.



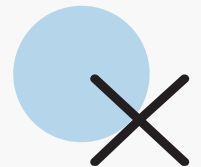
Decision making

Decision boards are needed and operate more effectively when a no-blame approach is taken, this culture can be better for long term remediation.



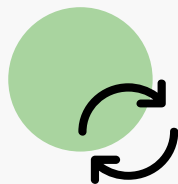
Island mode

Sites struggle to operate OT in 'island mode' with minimal business services - having not been designed with OT dependencies and security operations visibility in lieu of widespread IT outage.



Business continuity

Site business continuity and disaster recovery plans do not typically consider cyber outages, or the operational workarounds required to make, move and ship products or other necessary functions to support the site.



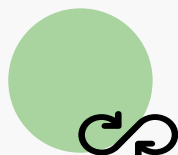
Manual workarounds

Alternative working practices and technologies may not be in place for weeks or months post-incident causing an increase in overtime and workplace stress.



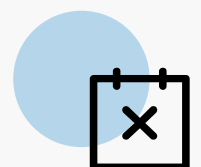
Supply chain

Third party support contracts are decentralised leading to inconsistent technology and security posture between sites and OT affecting what remediation and recovery activities can occur.



Recovery timelines

It can take weeks or months for business units, sites, and OT systems to get back to business-as-usual.



When preparedness failed: Examining real life case studies

The following three case studies are based on real life major cyber incidents. They each discuss how malware affected these organisations, what was observed from a technology perspective and how their businesses were impacted. Site architecture, technology implementation and management practices all played a pivotal part in how each incident developed. How would your business cope if faced with the following?

CASE STUDY 1

Enterprise-wide ransomware affecting production capability

Third party supply chain connections led to the introduction of malware into the Enterprise network, causing servers and workstations to be systematically ransomed region by region rendering them unusable.

Malware is indiscriminate and enterprise domain joined devices were exposed. Data and drives were encrypted with the immediate security operations response having an indirect impact on production capability. Most production sites lost access to site IT systems, the domain, WAN and remote access connections.

This led to the inability to access business systems, site information systems, and vendor connections severely hindering business operations globally. The critical need to isolate and segment operational technology environments was not implemented, leading to the lateral movement of malware.

Example technology issues:

- Inability for Manufacturing Execution Systems (MES) to operate in island mode.
- Overreliance on Virtual Private Networks (VPNs).
- No dedicated OT domain for critical systems (e.g. Human Machine Interfaces (HMIs), Application Servers, Database Servers, I/O Server, Historians etc.).
- Lack of alternative time services for OT systems.

Example response issues:

- Unavailable local data halted product shipment and affected warehouse space.
- Product quality was not monitored, increasing wastage and delays in shipment.
- Workarounds required, causing manufacturing to be slower for a significant period.
- Site information stored on the enterprise systems was unavailable for OT and impacted production.

Example operational challenges:

Risk management



Island mode



Business continuity



Manual workarounds



When preparedness failed: Examining real life case studies

CASE STUDY 2

Remote access breach to a site with interconnected sites and systems

A remote access connection introduced malware directly into sites and systems, grinding OT systems to a halt. The site had OT data connections to other regional sites and to a shared performance and regulatory repository within the organisation's IT environment.

The malware was able to cover up malicious activity meaning analysis and investigations were required to understand if critical OT systems had been compromised, and whether it had spread to site IT systems or to other sites.

Example technology issues:

- Undocumented assets, systems and connections between sites and systems.
- Gaps existed within incident response plans.
- Firewalls were configured to monitor WAN traffic, but not to manage OT data flows.
- Data repositories related to OT operations not considered as business critical.
- Significant variation in OT support contracts and expectations on vendors between sites.

Example response impacts:

- Sites were not prioritised which prevented stakeholders from effectively sequencing recovery and resulted in prolonged downtime.
- Communication plans between IT and OT stakeholders were ineffective leading to confusion and delayed remediation efforts.
- Vendors were unable to remotely access OT systems, increasing local support call outs.

Example operational challenges:

Governance



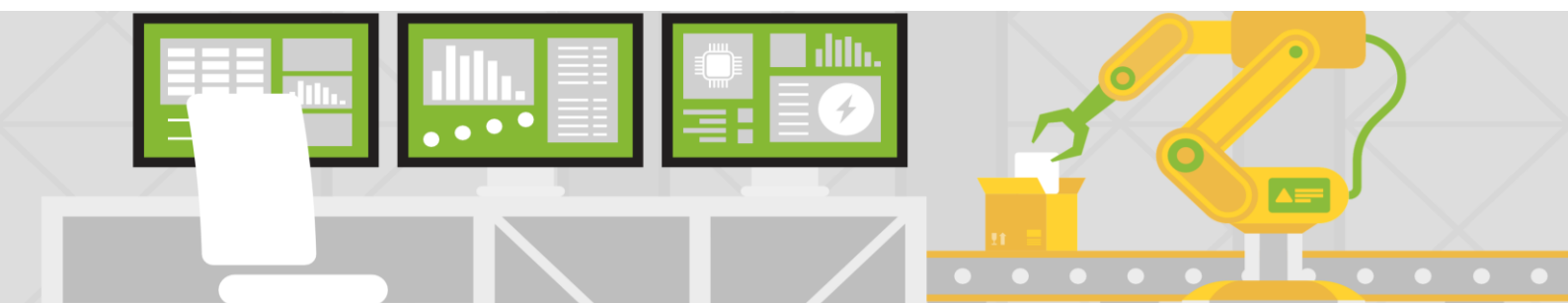
Information requirements



Decision making



Recovery timelines



When preparedness failed: Examining real life case studies

CASE STUDY 3

Malware affects OT systems on the shopfloor

An accidental or malicious user released malware directly into a critical site's systems. Multiple OT systems stopped working effectively. There was the potential for the malware to spread to Enterprise IT, other networks and other business units. The site shared infrastructure and facilities for employees, compounds and local warehouses.

The immediate focus was to get employee welfare systems and production fully operational. Some systems were cleaned and restored, while others remained offline. This meant that employees had to operate the plant with manual workarounds in place while containment, eradication and restoration services were ongoing.





Example technology issues:

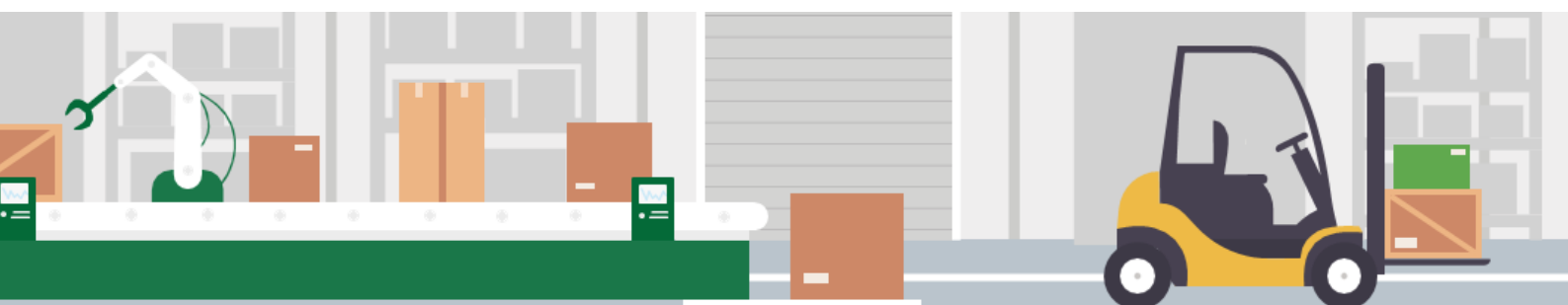
- No offline backups were stored for critical OT systems.
- Limited security zoning and network segmentation increased blast radius of malware (size of incident).
- Any cyber security controls implemented prior to the incident were ineffective – no testing of plans.
- No vendor remote access for critical support in 'island mode'.
- Unmanaged remote access connections direct to the shopfloor systems.

Example response impacts:

- Loss of unmanaged servers that were critical to operations.
- Employees worked additional overtime to continue operations manually.
- Extended production capability outage experienced due to physical safety concerns and a lack of logistics arrangements for technology and support staff.
- Due to limited network monitoring, identifying the attack vector took a significant amount of time which delayed response and recovery.

Example operational challenges:

Business continuity 	Physical damage 
Supply chain 	Manual workarounds 



When preparedness failed: Examining real life case studies

THE SCRAMBLE TO REACT

The impact of a cyber incident extends far beyond the immediate technical consequences. The experience of these events can leave a lasting psychological impact, with stress and anxiety persisting long after the technical recovery is complete.

Responding to a significant cyber incident involves many of the following:

- Locking down the networks
- Blocking data flow in and out of the business
- Protecting sensitive information
- Understanding the depth and breadth of the damage
- Rebuilding the processing environment

In parallel, a need to restore services as quickly as possible creates conflicting priorities and intensifies communications across the business.

When industrial sites are affected, different regional considerations, ownership models, business unit prioritisations and other motivations come into play. Often production sites are accountable for their local profitability and KPIs, operating as independent businesses within a wider organisation. Increasingly, disparities emerge between what is mandated centrally and the practices applied at local sites.

For example, it may be advantageous to 'protect the core' and lockdown enterprise IT services, however, this may significantly impact local sites, particularly those with a strong reliance on these critical services. The implications of a site being put in 'island mode' are generally not fully understood across the business. If technology and security controls are found to be lacking it can escalate quickly and investment decisions may be questioned. Furthermore, when people are stretched, wellbeing shouldn't be overlooked.

Cyber attacks are increasingly common and although major incidents that disrupt our lives are infrequent, these events should not be forgotten. Memory fades and investment wanes, even in organisations that have overcome catastrophic events.



Insights from major OT cyber incidents

Our teams have been deployed across the globe to support organisations and their business units restore production. From international ransomware outages to individual sites, we know what it is really like for those from the shopfloor to the boardroom during a time of crisis.

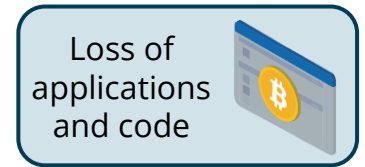
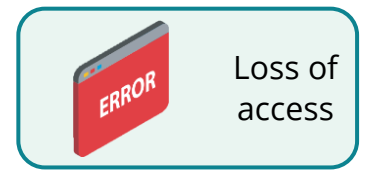
FACING THE REALITY ON THE SHOPFLOOR

Production systems have historically been isolated, off network and secured through obscurity of protocols. Today OT is increasingly connected throughout the business and technology stack which has changed the nature of how we respond to cyber incidents.

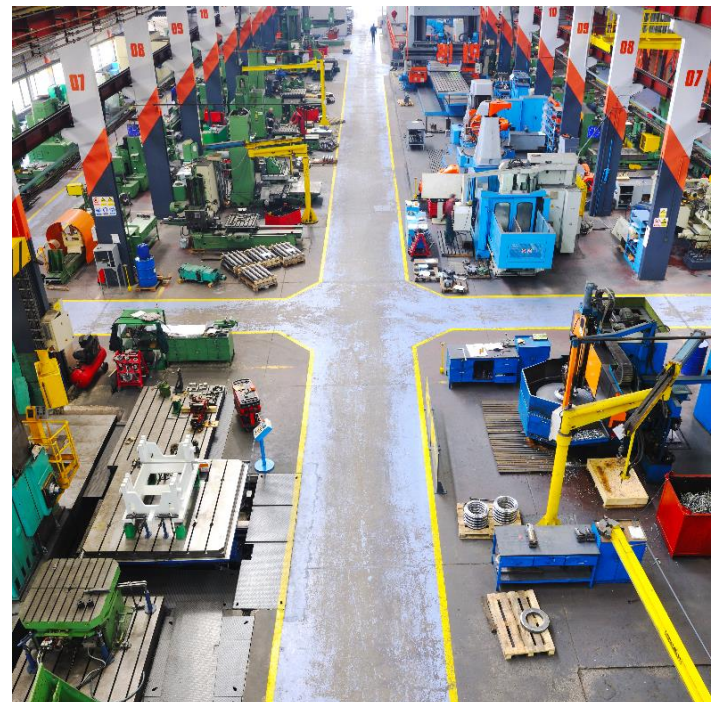
Being prepared is crucial for effective incident response. Understanding your assets and pre-determining management and recovery strategies will ensure you're ready to act decisively. Factors that affect the design and implementation of security and OT for industrial organisations also affect how a business responds to and recovers from significant technology outages.

These factors include:

- Productivity and safety focused environments, with 24/7 operations.
- Geographically distributed sites with remote warehousing and production facilities.
- Digital perimeters extend to third parties and cloud environments from the shopfloor.
- Legacy OT within the estate affects technology transition and integration.
- Multi-faceted management and governance for technology at sites that includes IT, operations, engineering, HSE and other functions.
- Limited centralised visibility of production information and security monitoring for OT.



Loss of control, view, access and applications and code are increasingly considered as potential impacts to OT – however the realisation that this can affect multiple systems and sites at the same time is lower on the radar. Systems and technology dependencies have crept into sites as OT is increasingly connected with applications and infrastructure using similar technology to IT. For example, domain and network services with differences in functionality or criticality are often overlooked. The consequences are often realised during disruption that can halt operations for significant periods.



Insights from major OT cyber incidents

SITE PERCEPTION VS REALITY DURING CYBER INCIDENTS

Perception and reality rarely match in everyday life. Speaking with one set of stakeholders can paint a very different picture once facts are checked on the ground. Unfortunately, any shortfalls are only amplified during an incident as time can be wasted in futile pursuits.

Perception	Reality
<p>“It’s an IT issue, IT are all over it?”</p>	<p>Cyber incidents impacting production are not just IT's problem. Understand the distinct security needs of IT and OT environments. Don't sideline OT teams – their expertise is crucial. Prioritise site-specific requirements when making risk reduction decisions.</p>
<p>“We already have security tools installed i.e. anti-virus software”</p>	<p>Security tools need more than just installation; they require ongoing maintenance and secure integration to be effective. Legacy technology in production environments often lacks robust security, demanding tailored solutions beyond standard IT policies.</p>
<p>“I can just contact the vendor.”</p>	<p>Local OT support contracts can create complexity during multi-site incidents. Prioritise vendor engagement to ensure timely support across impacted sites, especially given potential variations in technology and contracts.</p>
<p>“We didn’t even consider it was a cyber outage”</p>	<p>Recognising a cyber incident's impact on OT disruptions requires cyber security awareness and decisive action. Establish clear communication channels and pre-defined plans for incident response. Ask yourself: "What information is reliable during a cyber incident, and what steps should I take?" Prioritise both proactive planning and a security-first mindset.</p>
<p>“We need to secure the site; we’re doing it the IT way”</p>	<p>Applying blanket security controls across IT and OT environments, while seemingly efficient, can weaken overall security and disrupt operations. Over-integration can lead to unintended consequences, including operational issues, blurred responsibilities, and ultimately, a less secure environment.</p>

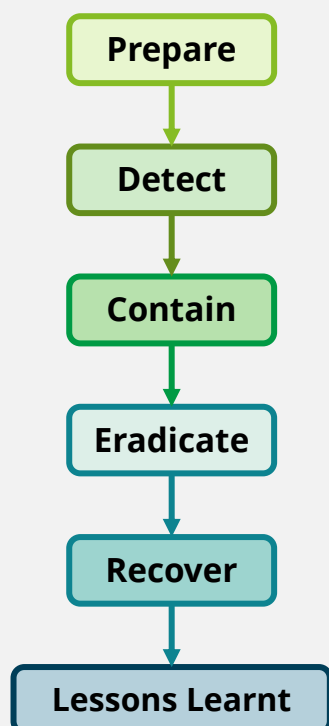
Be ready to boost your resilience and recoverability

OT has been in the cyber spotlight in recent years, and rightly so. The ever-changing threat landscape and increasing number of incidents impacting OT highlights that preparing for an outage should be a priority for every industrial organisation.

PREPARATION IS A CYBER PRIORITY

The “Prepare” stage is commonly overlooked within the OT environment. So, what does an organisation need to prepare for a cyber outage? How can you stop the spread of malware, minimise the disruption caused to your organisation and quickly have your production sites operating as if nothing had happened?

Cyber Incident Response Lifecycle



CONSIDERING ORGANISATIONAL NEEDS FROM ACROSS THE BUSINESS

Preparation should cover the interactions of people, processes, and technology to ensure they work together in a time of crisis. Given the cyber-physical nature of OT, the real-world impacts to health, safety, security, environment, and quality need to be considered. This allows policies and procedures to be optimised and security controls enhanced. Both local and organisational regulatory implications should be considered in cyber risk management and response planning.

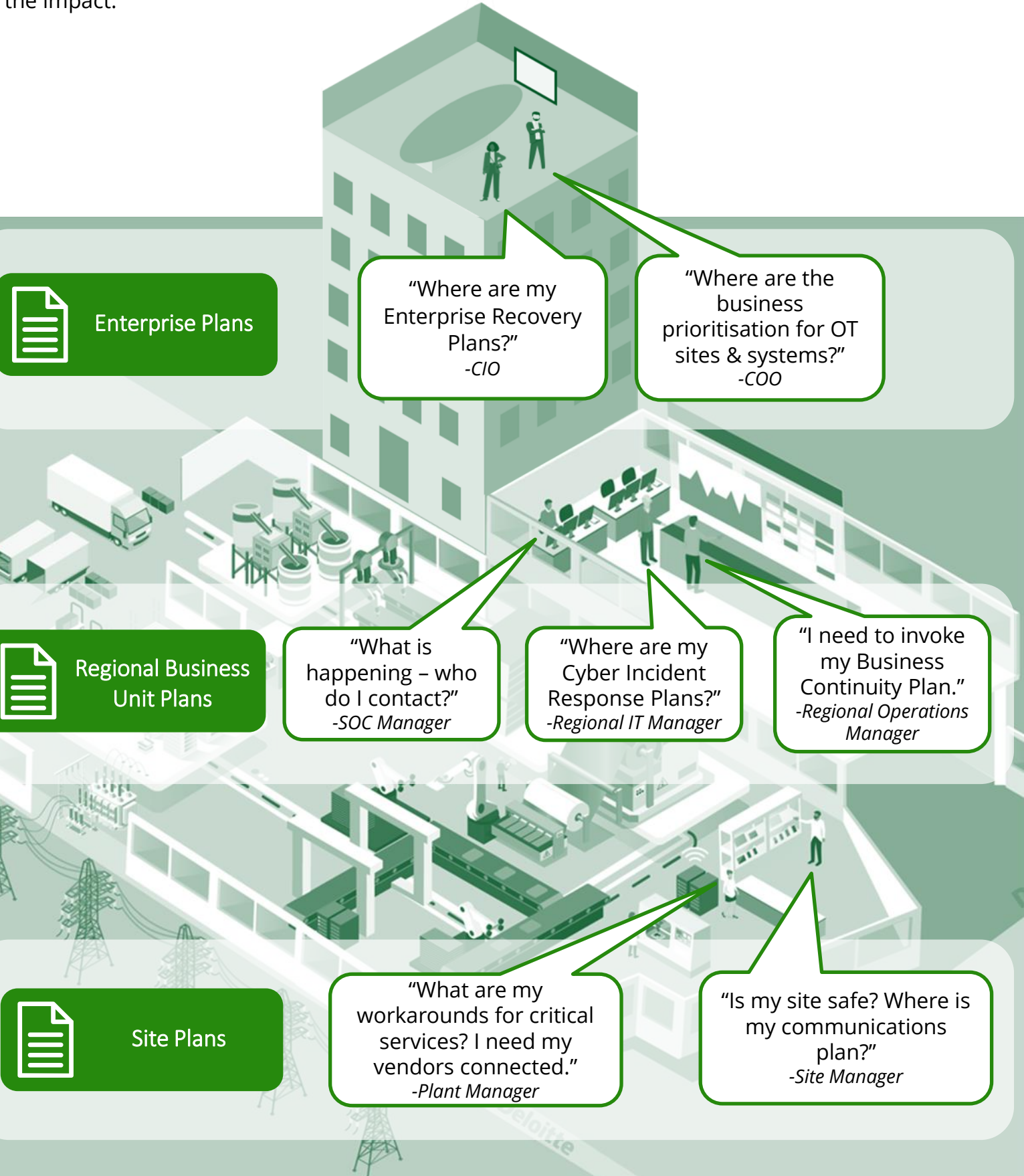
At **Enterprise levels**, response and recovery are typically covered by the organisation’s IT function, with security operation teams responding as technology and helpdesks alert to incidents within the estate. Enterprise IT focuses on the protection of critical infrastructure and applications at data centres and cloud environments, extending to IT infrastructure and services at sites and in hub locations.

Often the IT function has further support at **Business Unit** and **Regional** levels, with hands on and local coverage for sites and service management.

At **Site** level, the primary focus is safety and keeping production systems running. Preparation is required for both the IT and OT functions with consideration for areas of convergence, roles, and responsibilities. The drivers and motivations for the site are key when prioritising remediation and recovery activities.

Be ready to boost your resilience and recoverability

Preparation provides guidance to what is needed in a crisis and readies your response to reduce the impact.



Conclusion

PREPARING FOR THE FUTURE

Proactive measures for industrial cyber security are important now more than ever. Based on our extensive experience in working with OT clients in preparing and responding to cyber attacks, the following are key actions you should consider now to reduce your risk:

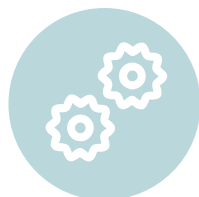
Map your critical business processes to assets
Review disaster recovery plans
Ensure compromised vendors and/or supplier scenarios are considered
Prepare for network disconnection scenarios to maintain operations
Keep up-to-date, offline digital and physical backups of critical OT systems
Protect the most critical assets.

Effective OT cyber security requires acknowledging and addressing the unique challenges inherent in these environments. The following considerations are crucial when designing and implementing security controls for OT:



Recognising the unique risks of OT

It is a common misconception that cyber threats to OT systems are mitigated by enterprise or IT security measures. As technological advancements bring IT and OT domains closer together, it is crucial to recognise that they remain distinct areas with unique risk profiles.



Embracing the complexity of cyber incidents

We acknowledge the complexity and uniqueness of each business – every incident is distinct due to a diversity of systems and architectures. Effective preparation requires close collaboration between IT and OT teams to align business needs with robust security practices.



Take action today

Proactive measures are essential. Don't wait for a cyber incident to test your defences. We can help develop and implement effective strategies to protect your critical infrastructure. Together, we can build a secure future for your organisation.

Your partner in cyber resilience

We are committed to supporting your journey toward robust cyber resilience. By adopting our insights and collaborating with our experts, you can enhance your preparedness and safeguard your business against emerging threats.








How we can help

Through extensive experience in Cyber Incident Response, we have developed a comprehensive set of services which build Digital Resilience and improve Enterprise Recovery preparedness. The response and recovery from catastrophic cyber incidents can be quick, efficient and less financially damaging if organisations invest in recoverability, as opposed to waiting to react.

PREPAREDNESS ACTIVITIES

Preparing for a catastrophic cyber attack is an all-encompassing journey

Before an incident, organisations can increase preparedness for a catastrophic cyber attack. Our approach to achieve this looks across five key pillars that should all be considered to increase overall readiness. These services look to enable organisations to reduce the impact of an incident and enable a quicker return to business as usual.

	Description	Example services
 Prioritised recovery planning	Plans for recovery that are prioritised and based on business criticality	<ul style="list-style-type: none"> Process and technology mapping Disaster recovery plans and playbooks
 Building blocks of recovery	Actual recovery tools and materials in place to rebuild the organisation	<ul style="list-style-type: none"> Backup architecture Data vaulting solutions
 Burst capacity	Ability to scale up/down resources where they are scarce/excessive	<ul style="list-style-type: none"> Scenario based business continuity plans Third party and vendor assessments
 Organisational readiness & alignment	Crisis team, procedures and processes enabling an enterprise-wide recovery	<ul style="list-style-type: none"> Crisis exercising Testing of backups, disaster recovery plans, and playbooks
 Minimise blast radius	Security and architectural thinking to reduce the reach of an incident	<ul style="list-style-type: none"> Architecture design and reviews Security tools and system hardening

While establishing robust cyber defence is essential, it's equally crucial to acknowledge that no system is entirely impenetrable.

When a cyber attack does occur, a swift and strategic response can mean the difference between minimal disruption and potentially catastrophic consequences.

REACTIVE ACTIVITIES

Recovering the business after a catastrophic cyber attack requires a breadth of capabilities

In the aftermath of an incident technical expertise is key. However, it is not the only area in demand. Capabilities across a multitude of areas is vital. Legal, people leadership, communications, forensics and crisis management are examples of the skills required. We have the breadth and depth of experiences supporting organisations across the phases of an incident:

 Respond	 Recover	 Transform
<ul style="list-style-type: none"> 24/7 Incident response: incident triage, analysis, containment Incident leadership: strategic level guidance; a trusted partner Recovery strategy: strategy and journey to recovery 	<ul style="list-style-type: none"> Business driven: identifying what is critical to the business Recover securely: recover technology to a secured state Future planning: reduce the likelihood of a further breach 	<ul style="list-style-type: none"> Risk identification: focus on the key risks to the organisation Build foundations: foundations for a more resilient, future state Transformation: a business wide strategy to continue uplift

Contact us

Drop us a note to get the conversation started and to discuss your Digital Resilience and Enterprise Recovery journey.



Sydney Grenzebach

sgrenzebach@deloitte.co.uk

Partner
Sponsor



Nick O'Kelly

niokelly@deloitte.co.uk

Partner
Sponsor



Anna Burrell

aburrell@deloitte.co.uk

Director
Author



Jonathan Lam

jdlam@deloitte.co.uk

Senior Manager
Author



Ivelina Koleva

ivelinakoleva@deloitte.co.uk

Partner
Contributor



Lynne O'Hara

lohara@deloitte.co.uk

Director
Contributor

Other acknowledgments

Thanks to Daniel Usman, Edward Meadowcroft, Liam Sullivan and Waqar Sheikh





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please [click here](#) to learn more about our global network of member firms.