KUDELSKI SECURITY

Building OT Resilience: Governing Cyber Crisis in Industrial Operations

Alyssa Fleck
Strategy, Risk & Compliance Consultant

An OT crisis does not start when a PLC fails, it starts when no one knows who is in charge, or what to shut down.

In industrial environments, a single misstep, a faulty sensor, a remote access left open can trigger a major crisis in seconds. It is fast, it is stressful, and often, it takes everyone by surprise. Because OT crisis management is not just technical. It is human. And when everything is at risk, clarity and coordination make all the difference.

Critical Challenges in OT Cybersecurity

In an OT environment, there is no room for downtime. An interruption can compromise both production and human safety.

The core challenge in managing OT cyber crises is governance. Without clearly defined roles and responsibilities **(who does what and when)**, quickly mobilizing the right stakeholders becomes chaotic, which leads to delayed or inadequate responses. Effective crisis management requires a documented RACI model that includes both corporate teams (CIO, cybersecurity, legal, communications, etc.) and local OT actors such as plant managers, maintenance leads, and OT champions who deeply understand operational processes.

However, aligning these diverse stakeholders is rarely straightforward. Strong management sponsorship is essential to ensure coordination, accountability, and decision-making at the right level. although ensuring it remains a persistent challenge for many organizations.

This governance structure is essential because critical decisions like isolating or shutting down an asset or system must be validated by the user operating the system, not only the owner. These decisions carry serious safety, contractual, and operational implications that governance helps manage responsibly.

This organizational clarity is even more critical given the technical challenges of IT/OT convergence. Attackers increasingly leverage weak points in the network to penetrate OT environments. For example:

- Poorly secured Wi-Fi or inadequate network segmentation can allow lateral movement from IT to OT systems.
- Legacy OT protocols (e.g., Modbus) typically lack encryption and authentication, making them highly vulnerable to manipulation.
- Traditional IT security tools such as SIEMs are not well designed or incorrectly implemented for industrial systems. They often lack visibility into proprietary protocols and can even disrupt sensitive processes.

To detect and respond effectively, organizations must adopt specialized OT cybersecurity solutions like industrial IDS/IPS (e.g., Claroty, Nozomi, etc.) that understand operational contexts and can monitor critical assets without causing disruption.

Without strong governance guiding rapid, informed decisions aligned with these technical realities, incident response risks being fragmented and ineffective, jeopardizing safety and production continuity.

Understanding the Technical and Operational Risks of OT Cyber Incidents

In an OT environment, a cyber crisis is never just an IT incident. It disrupts production, impacts operational and human safety, exposes the organization to regulatory non-compliance, and can cause significant financial losses within hours.

In systems designed for continuous operation, even the slightest downtime is unacceptable. Yet, too often, OT crisis management maturity is insufficient, due to a lack of real anticipation or inadequate field-specific preparedness.

From a technical perspective, an attack can lead to a loss of network communication, rendering control systems inoperative. PLCs, RTUs, can be stopped, reprogrammed, or hijacked, directly compromising industrial processes. SCADA systems and operator workstations are frequent ransomware targets, leading to the paralysis of supervisory capabilities. Attackers may also implant persistent backdoors or falsify sensor and actuator data, disrupting process control and creating hazardous conditions.

These risks are exacerbated by the widespread use of unsecured protocols, lack of proper network segmentation, and poorly managed IT/OT convergence, which together increase the attack surface and complicate incident containment.

Key Actions for Building OT Resilience

Effective cyber crisis management in OT environments requires prioritizing key actions in governance, preparation, collaboration, and continuous improvement:

Governance:

- Ensure strong executive sponsorship to support alignment, decision-making authority, and cross-functional coordination.
- Define a dedicated OT Cybersecurity Responsible to oversee cyber risk management and incident response.
- Conduct Business Impact Analyses and OT-specific risk assessments to prioritize mitigation efforts effectively.
- Establish clear service-level agreements with third-party providers to ensure accountability.

Preparation:

- Know your industrial environment by assessing critical processes and identifying their owners.
- Use specialized ICS tools alongside traditional IT security solutions for comprehensive protection.
- Implement strong security controls, including network segmentation, to contain threats and limit lateral movement.
- Secure remote access and maintain detailed operational knowledge to detect anomalies quickly.
- Evaluate suppliers and third parties to understand and mitigate potential risks.

Collaboration & Documentation:

- Promote close collaboration between IT and OT teams and involve external stakeholders such as vendors and emergency responders (CSIRT).

- Develop and regularly update Business Continuity Plans, Incident Response Plans, and Disaster Recovery Plans tailored to OT environments.
- Clearly define roles, responsibilities, and communication protocols to ensure smooth coordination during incidents.

Testing & Continuous Improvement:

- Regularly test crisis response plans through realistic simulations and tabletop exercises.
- Incorporate lessons learned to continuously refine security posture and response capabilities.

Closing the Gap Between OT Risk and Readiness

Resilience in industrial cybersecurity is not built in the heat of a crisis, it's forged through governance, preparation, and collaboration long before an incident occurs. In OT environments, where downtime can endanger both human lives and operational continuity, crisis response must go beyond technical containment. It must be driven by clarity of roles, alignment between IT and OT stakeholders, and the readiness to make fast, informed decisions that balance safety, business continuity, and accountability.

Governing an OT cyber crisis starts with recognizing that people, not just technology, are central to effective response. Strong executive sponsorship, documented responsibilities, and the ability to coordinate across disciplines are what turn reactive firefighting into proactive resilience.

By investing in specialized OT tools, robust processes, and cross-functional crisis exercises, organizations can navigate disruptions with confidence and minimize long-term impact.

The future of industrial operations depends on bridging the gap between operational realities and cybersecurity best practices. Governing OT cyber crises is not optional, it's a strategic imperative.

The time to build that resilience is now.

Alyssa Fleck

About the Author

Alyssa is a Strategy, Risk & Compliance Consultant at Kudelski Security, where she focuses on IT and OT security assessments (Maturity & Risk), incident response planning, and business continuity management, crisis simulations and tabletop exercises.
She holds a Master's degree in Law and Security of Information Technologies from the University of Lausanne and EPFL (The Swiss Federal Technology Institute), and a Bachelor's in Management from HEC Lausanne.

Before joining Kudelski Security, Alyssa worked in the banking sector, where she developed a strong foundation in IT risks and controls.
Her expertise has since expanded to include maturity assessments and OT security. Her extensive experience spans a diverse range of industries, including finance, luxury, industrial, and retail sectors, where she helps organizations understand their risk landscape and build practical, resilient security strategies tailored to their specific needs.

KUDELSKI SECURITY