What OT Security Incidents in 2025 Taught Us About Remote Access

eBook by

Introduction

Remote access has become one of the most consequential attack surfaces in industrial environments, not because it exists, but because of how it's implemented.

In 2025, organizations across manufacturing, energy, and utilities experienced firsthand how remote access pathways intended to keep operations running can just as quickly bring them to disrupt operations. From production shutdowns to public safety threats, security incidents repeatedly traced back to the same root cause: remote access architectures built for convenience rather than control.

The 2025 OT Threat Landscape at a Glance

According to a SANS Institute survey[1], 22% of organizations experienced an OT security incident in the past year, and 40% of those incidents led to operational disruption. These numbers reveal just how exposed industrial environments have become. But what was the major reason for these incidents? Half of all reported incidents stemmed from unauthorized external access, while only 13% of organizations had advanced controls such as session recording or OT-aware access in place.

22%

Experienced an Incident

of organizations reported an OT security incident in the past year.

40%

Led to Disruption

of those incidents resulted in operational disruption.

50%

Unauthorized Access

of all reported incidents stemmed from unauthorized external access.

13%

Advanced Controls

of organizations had session recording or OT-aware access controls in place.

© 2026 Xona Systems, Inc. All rights reserved.

Three OT security incidents in 2025 that exposed vulnerabilities

In 2025, organizations across manufacturing, energy, and utilities experienced firsthand how remote access pathways intended to keep operations running can just as quickly bring them to disrupt operations. From production shutdowns to public safety threats, security incidents repeatedly traced back to the same root cause: remote access architectures built for convenience rather than control.

1. Jaguar Land Rover's Manufacturing Shutdown

A cyberattack triggered a **month-long shutdown** across Jaguar Land Rover's global manufacturing operations, costing the company an estimated **$1.7 to $2.4 billion in lost revenue**. According to Dark Reading [2], the attackers had likely remained inside JLR's systems from a previous breach, making the ransomware incident far more severe. JLR initially shut down operations "proactively," but later disclosed that customer data had been compromised.

Critical Failure Points

Weak identity governance allowed attackers to persist undetected

Limited enforcement of segmentation boundaries enabled lateral movement

Lack of real-time monitoring meant the attack wasn't caught until it was too late

© 2026 Xona Systems, Inc. All rights reserved.

2. Nucor's Production Halt

Steel manufacturer Nucor Corporation identified a cybersecurity incident involving **unauthorized third-party access** to certain IT systems used by the company [3]. Nucor temporarily and proactively halted certain production operations at various locations [4].

Critical Failure Points

Unauthorized third-party access to IT systems went undected

Lack of early detection and containment capabilities allowed the incident to escalate

Poor visibility and segmentation across environments made it difficult to isolate the threat

3. Florida Water Treatment System Hacked

A hacker **gained remote access** to a Florida city's water treatment system and attempted to **poison the water supply** by drastically increasing the level of sodium hydroxide, a chemical used to control acidity [5]. The attack briefly altered the chemical settings before an operator spotted the change and reversed it, preventing harm.

© 2026 Xona Systems, Inc. All rights reserved.

Critical Failure Points

Lack of detection and alerting left the system vulnerable to manual intervention

Excessive user permissions granted unnecessary control over critical systems

Out-of-date critical control infrastructure lacked basic security hardening

Common Vulnerabilities Across OT Security Incidents

Vulnerability	Solution
Unauthorized Third-Party or External Access	Replace direct network access with a brokered remote access model that authenticates users before establishing any connection to OT systems. Require strong identity checks, eliminate shared credentials, and ensure vendors only connect when needed, to only the systems required, and for a limited time.
Operational Shutdown Triggered by Cyber Intrusions	Build the ability to quickly revoke access during an incident, isolate critical systems remotely, and continue operations safely while investigations and recovery take place.
Over-Privileged Accounts & Weak Access Controls	Shift from permanent access to just-in-time, task-based authorization. Users receive only the minimum access required, only for the duration of approved work, eliminating standing credentials and reducing the impact of stolen or misused accounts.

© 2026 Xona Systems, Inc. All rights reserved.

Insufficient Monitoring & Lack of Early Detection	Enforce session-level visibility to capture who accessed what, when, and how — enabling immediate detection of suspicious behavior and accelerating investigation before safety or production is impacted.
Poor Segmentation Between Systems	Require separation through controlled access boundaries rather than flat connectivity. Remote users interact only with approved assets or services, preventing lateral movement across IT, OT, and control environments, even if a session is compromised.
Critical Infrastructure Not Hardened for Cyber Threats	Remove legacy remote tools, outdated systems, and insecure configurations from critical environments. Harden engineering workstations, HMIs, and remote access entry points so even legitimate access cannot be easily abused or repurposed by attackers.

Why These Patterns Persist

Across manufacturing, utilities, and critical infrastructure, these incidents share a common cause: **IT-style remote access models are being applied to OT environments they were never designed to protect.**

The Core Problem

As OT systems become more connected and reliant on remote support, attackers increasingly exploit the same access paths engineers use to keep operations running. When remote access lacks clear boundaries, visibility, and control, small gaps can quickly escalate into operational disruption.

© 2026 Xona Systems, Inc. All rights reserved.

Remote Access Remains Essential in 2026

Remote access itself is not the problem; it is an operational necessity.

- **Engineers Rely on It**

  Engineers depend on remote access for rapid troubleshooting and recovery. When a system goes down, the ability to diagnose and resolve issues remotely is often the difference between a minor delay and a costly production halt. Removing remote access is not a viable option.

- **Vendors Depend on It**

  Vendors depend on remote access to support specialized systems that cannot always be maintained on site. OEM support, firmware updates, and diagnostics for complex industrial equipment frequently require remote connectivity, often from third parties with deep system-specific expertise.

The challenge is not choosing between security and availability, but delivering remote access in a way that supports both.

© 2026 Xona Systems, Inc. All rights reserved.

Foundational Principles for OT-Safe Remote Access

These principles move remote access away from convenience-driven design and toward **intentional, risk-aware architecture** addressing the root causes exposed by the 2025 incidents.

Least Privilege by Default

Access should be granted only to the specific systems, functions, and timeframes required to perform a task, nothing more. Broad network access or standing privileges dramatically increase risk.

Just-in-Time Access

No standing access. Permissions are issued per task and removed immediately after use.

Explicit Trust Boundaries

OT environments should never assume trust based on network location alone. Every remote connection, whether from internal staff or third parties, must be authenticated, authorized, and monitored.

OT-Aware Controls

Security mechanisms must account for legacy systems, fragile devices, and operational constraints, avoiding controls that could disrupt processes or introduce safety risks.

© 2026 Xona Systems, Inc. All rights reserved.

How Compliance Reinforces OT-Safe Remote Access

Well-designed remote access controls directly support compliance objectives by answering the questions auditors and regulators consistently ask: *Who has access to OT systems? Why was access granted? What systems were accessed, and for how long? How is access monitored, reviewed, and revoked?*

Remote Access Principle	Operational Benefit	Compliance Outcome
Least privilege by default	Users and vendors access only what they need	Clear authorization boundaries; reduced audit findings for over-permissioned access
Just-in-time, time-bound access	No standing or always-on connections	Demonstrable control over access duration and purpose
Explicit trust boundaries	Connections authenticated and authorized regardless of location	Alignment with zone-and-conduit and zero-trust expectations in OT standards
OT-aware controls	Security that does not disrupt safety or operations	Evidence of risk-based, fit-for-purpose security design
Session monitoring & logging	Visibility into active and historical access	Audit-ready records for investigations and regulatory reporting

© 2026 Xona Systems, Inc. All rights reserved.

Conclusion: Rebuild Remote Access on the Right Foundation

The 2025 incidents reveal a single point of failure: remote access built for convenience, not security. Unauthorized entry, over-privileged accounts, blind spots in monitoring, and weak network segmentation gave attackers an open door.

The answer isn't to eliminate remote access. It's to rebuild it on four principles: least-privilege by default, just-in-time access, explicit trust boundaries, and OT-aware controls.

Organizations that act now won't just avoid becoming the next headline. They'll turn remote access from their greatest vulnerability into a defended advantage.

---

[1] SANS Institute Survey, Industrial Cyber, 2025
[2] Dark Reading – JLR Cyberattacks, 2025
[3] [4] Industrial Cyber / SC Media – Nucor Incident, 2025
[5] BBC News – Florida Water System Hack, 2021

© 2026 Xona Systems, Inc. All rights reserved.

Take the Next Step

Connect with Secure Remote Access Experts for OT Environments. Learn how Zero Trust remote access can strengthen your OT security posture while improving operational efficiency.

Visit **www.xonasystems.com** to learn more or **schedule a demo** with our OT security specialists.

About Xona Systems

Xona Systems provides Zero Trust secure remote access built specifically for operational technology and critical infrastructure environments. The Xona Platform replaces VPN-based access with identity-driven, least-privilege control, full session visibility, and audit-ready accountability, without exposing OT networks or disrupting operations. **www.xonasystems.com**