Operational resilience in the age of connectivity

New research on cyber readiness in connected manufacturing environments

Rockwell Automation

The new reality of OT Security

Industrial companies are connecting more systems, scaling AI faster, and pushing operations to move in real time. Those investments create speed and flexibility. They also expand operational risk.

New Rockwell Automation data shows a disconnect between confidence and operational exposure.

Nearly half of organizations (46%) experienced a cyber incident in the past year, yet 90% say they are confident they can contain a cyber incident. More than one-third (34%) identify cybersecurity as one of the biggest external obstacles to growth over the next 12 months.

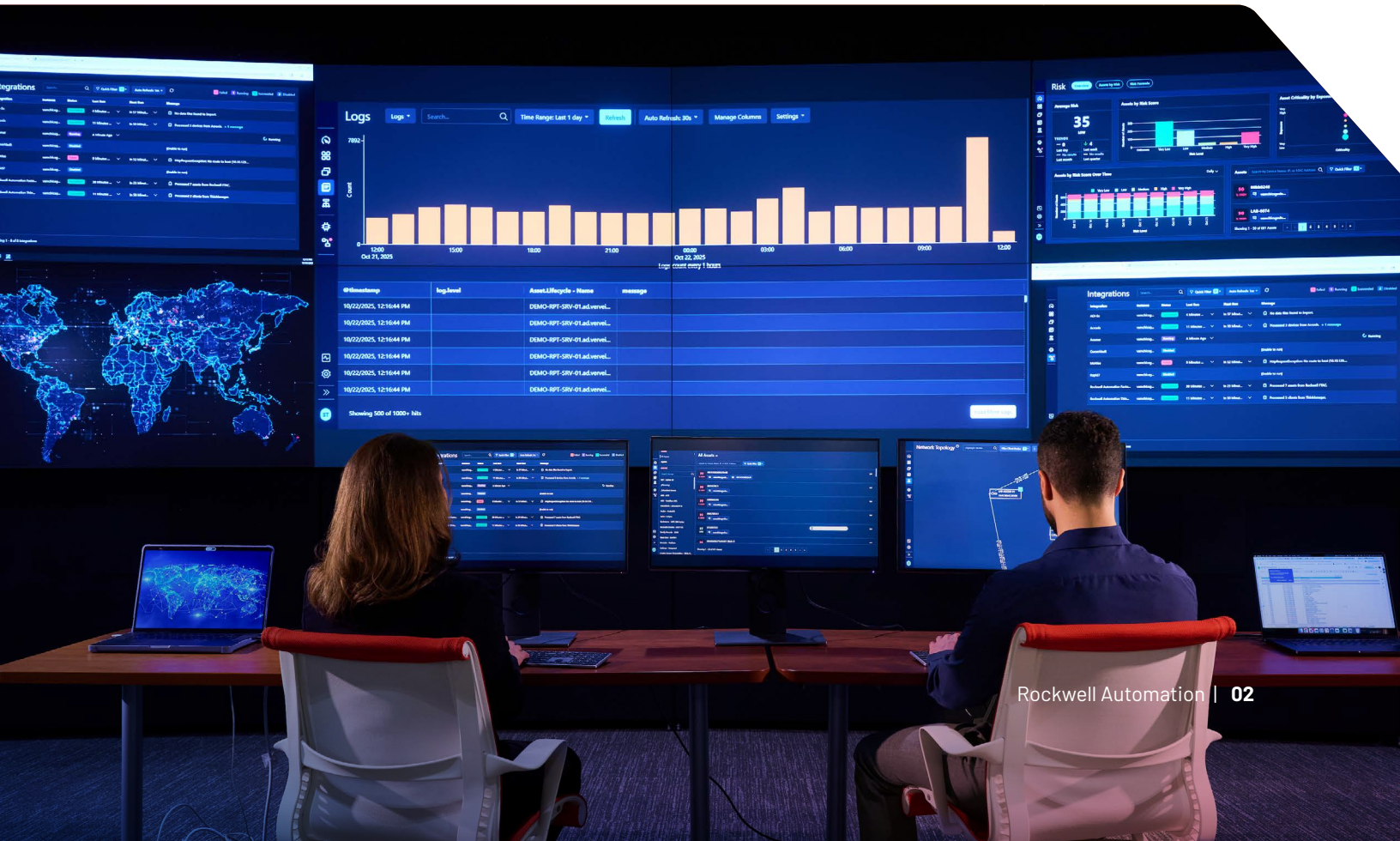
Despite this, organizations understand the stakes and are taking action to build their resilience – and confidence. 62% have already invested in cybersecurity platforms such as asset inventory, intrusion detection systems, and secure remote access. Cybersecurity also ranked among the top technologies delivering ROI over the past 12 months.

The issue is not awareness. Industrial organizations know cyber risk affects uptime, continuity, productivity, and growth. The challenge comes from securing operations that continue to grow more connected and more complex.

AI adoption continues to rise. IT and OT environments continue to converge. Operational data moves across more assets, users, devices, and applications than ever before. Every connection creates another dependency. Every dependency creates another point of exposure.

The good news is that organizations are rising to the challenge. They no longer treat cybersecurity as a separate IT initiative but are instead increasingly viewing it as part of operational performance.

The companies leading the next phase of industrial operations will be those that build visibility, secure architecture and response capabilities that keep production moving during disruption.



Growing confidence through investment – but is it enough?

Organizations are not standing still. They're investing in the technologies, architectures and capabilities needed to strengthen cyber resilience. The next step is bringing those investments together into a cybersecurity program that continuously improves visibility, reduces risk and adapts to evolving operational needs. The data shows where organizations are focusing today.

Key findings include:

- IT/OT integration points are ranked as one of the most vulnerable to cyber incidents, just behind IT systems/enterprise networkssay cybersecurity investments delivered among the highest ROI over the past 12 months
- Cybersecurity is the second-leading ROI driver among technology investments

These findings point to a clear shift: organizations are embedding cybersecurity into broader digital transformation strategies alongside AI, automation, cloud technologies and connected operations. But as environments become more interconnected, resilience depends on how well organizations can translate investment into coordinated action.

62%

have already invested in cybersecurity platforms

45%

plan to use AI and machine learning for cybersecurity over the next 12 months

35%

More than one-third of industrial organizations identify cybersecurity as one of the biggest external obstacles to growth – second only to workforce shortages over the next 12 months

37%

say securing IT/OT architecture will drive positive business outcomes over the next five years

Building resilient OT operations

Industrial companies have made significant progress investing in cybersecurity. The next challenge is turning those investments into operational resilience.

Resilient OT security requires more than tools and point solutions. It requires a proactive, end-to-end approach aligned to globally recognized frameworks and standards such as NIST, NIS2 and IEC 62443. This gives organizations a structured way to improve security maturity while meeting regulatory requirements.

The following capabilities highlight actions taken by leading organizations and show what that looks like in practice.

Strategic advisory

Build a risk-based cybersecurity strategy

Cybersecurity resilience starts with understanding risk in the context of operational priorities, business objectives and organizational reality. Before organizations can effectively reduce risk, improve resilience, or meet compliance requirements, they need a clear view of their current cybersecurity posture and the gaps that present the greatest impacts. Without that foundation, cybersecurity investments can become fragmented, reactive and difficult to operationalize.

Organizations that implement strategic advisory services can:

- Identify risks, establish priorities, and align investments with business outcomes
- Replace reactive, ad hoc security decisions with a prioritized, risk-based roadmap aligned to operational and business objectives
- Understand current exposure across assets, vulnerabilities, processes and governance practices, enabling resources to be focused where they will have the greatest impact
- Improve compliance readiness by identifying security gaps and aligning remediation efforts to applicable standards and requirements
- Build internal alignment across IT, OT and leadership around a shared understanding of risk, priorities and measurable security outcomes

Industrial networking and infrastructure

Organizations continue to modernize IT/OT architecture as operations become more connected. While each new connection increases cyber risk, a defensible architecture helps prevent complexity from becoming an expanded attack surface. Leading organizations that embed cybersecurity into the design of their operations are better positioned to reduce risk, improve resilience and spend less time responding to incidents and more time driving operational outcomes.

Proactive organizations can:

- Advance digital transformation initiatives with confidence while helping protect critical operational systems
- Reduce the likelihood and impact of disruption through network segmentation to contain threats before they affect production
- Enable secure remote access that supports operational flexibility, productivity and collaboration without creating unmanaged entry points
- Implement secure-by-design architectures that reduce risk across the asset lifecycle
- Reduce long-term security costs by proactively addressing risk through architecture and design rather than reactive remediation

Asset inventory & lifecycle management

Gain visibility into assets and risk

Limited visibility is one of the most common barriers to building resilience. Without a complete view into the environment – including legacy systems, serially connected devices or temporary connections – organizations lack the starting point needed to plan and execute meaningful risk reduction.

Comprehensive asset visibility enables organizations to:

- Understand and prioritize cyber risk across the operational environment
- Reduce blind spots that can create operational, safety and cybersecurity risk
- Make faster, more informed decisions by understanding which assets are connected, which are exposed to risk and which are most critical to production and business operations
- Accelerate risk reduction efforts by prioritizing remediation activities based on operational impact, not just vulnerability severity
- Improve operational resilience through continuous asset lifecycle management that helps maintain a secure and supported environment over time
- Rely on the program foundation to build upon compensating controls and other components for end-to-end cybersecurity

Risk and vulnerability management

Prioritize and remediate the risks that matter most

Organizations cannot eliminate all cyber risk, but they can improve security posture by strengthening how quickly they identify, prioritize and respond to threats before they impact operations. As industrial operations become more connected, effective risk management depends on contextual visibility, risk-based decision making and sustaining operational continuity through disruption.

A risk-based vulnerability management program helps organizations:

- Prioritize remediation based on operational impact, not just severity scores
- Reduce mean time to remediation across OT assets
- Demonstrate measurable compliance progress against IEC 62443, NIST CSF and NIS2
- Enable informed investment decisions by aligning cybersecurity investments to business risk tolerance and operational objectives

Managed detection and response

Maintain continuous awareness across operations

As IT and OT environments become increasingly interconnected, organizations face a growing challenge in distinguishing routine security events from threats that could disrupt operations. Continuous monitoring helps understand the risks that matter most before they cause disruption.

A proactive detection and response program helps organizations:

- Accelerate detection and response by maintaining 24/7 monitoring and continuous visibility across IT and OT environments
- Enable faster, more informed decision-making with contextual insight that helps teams understand which threats need immediate action
- Close the skills gap by extending internal capabilities with dedicated OT security expertise without the cost of building and maintaining a full in-house SOC
- Strengthen the effectiveness of the program by integrating threat detection with vulnerability management, incident response, governance and continuous improvement efforts

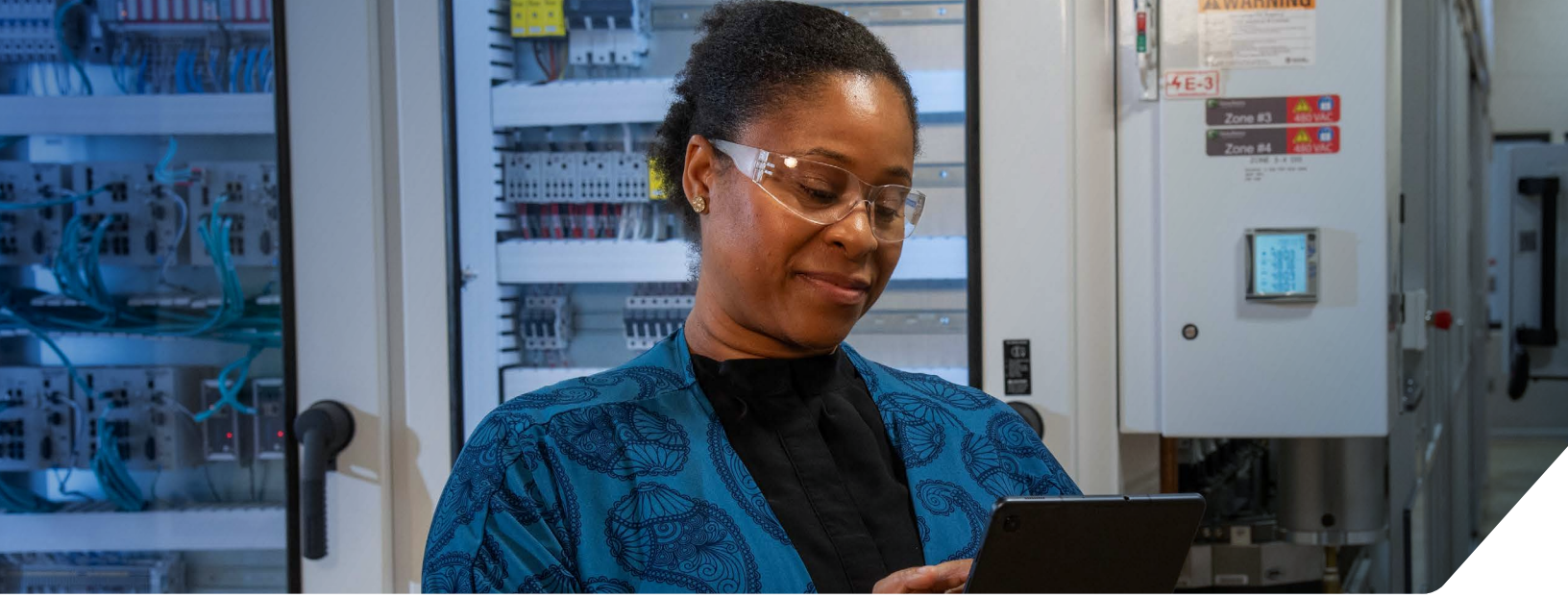
Incident response & recovery

Contain, restore and improve

When a cybersecurity incident occurs, a quick response is critical in determining how much damage, downtime and cost an organization may face. Containing an incident is only part of the challenge. Organizations must understand the importance of recovery readiness when it comes to operational resilience. When the worst happens, they need the ability to restore services quickly and return to normal operations.

A mature incident response program enables organizations to:

- Reduce the impact of cyber incidents through pre-defined, tested response and containment procedures
- Accelerate operational recovery by coordinating response and recovery across IT, OT and operational teams
- Minimize downtime by improving recovery readiness for critical systems
- Strengthen stakeholder trust through clear communication, governance and incident management during and after an event
- Develop a detailed incident investigation to identify root cause and apply lessons learned to continuously strengthen cyber resilience



Resilience is becoming a competitive advantage

Industrial organizations are investing heavily in cybersecurity, AI and connected operations. Those investments are increasing confidence, but technology alone does not create resilience.

The organizations that gain the most value from cybersecurity will be those that take a proactive, programmatic approach. By building visibility, risk-based decision making, secure architectures, continuous monitoring and recovery readiness into their operations from the start, they can reduce operational risk, sustain production and enable the business to move forward with confidence.

In a more connected industrial environment, cybersecurity is no longer only about protecting assets. It is about enabling resilient operations that can adapt, recover and continue delivering business value.

To learn more contact your Rockwell Automation representative.

Rockwell Automation

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2663 0600
ASIA PACIFIC: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
UNITED KINGDOM: Rockwell Automation Ltd., Pitfield, Kiln Farm, Milton Keynes, MK11 3DR, United Kingdom, Tel: (44) (1908) 838-800

Publication GMSN-SP043A-EN-P - August 2026