2026 OT Cybersecurity benchmark report

OT security scope expands to include facility, safety and physical security systems.

Honeywell Technologies

About the report

The **Honeywell Technologies 2026 OT Cybersecurity benchmark report** shows where security coverage is breaking down across connected systems and which visibility, monitoring and recovery practices are associated with faster diagnosis and shorter downtime. The findings help security leaders benchmark current maturity and prioritize capabilities that can strengthen resilience before disruption occurs.

About the survey

The benchmark study was fielded in May and June 2026, capturing the views of 603 respondents: CISOs and OT security leaders, compliance and risk executives, plant and operations managers, and cybersecurity architects.

Respondents represent critical infrastructure sectors where a cyber disruption can affect production, safety, recovery and revenue, including oil and gas, energy and utilities, maritime, healthcare and manufacturing, with participation across the Americas, EMEA and APAC. Unless otherwise noted, the findings reflect respondents' self-reported practices, experiences and assessments.

Table of contents

Overview

Key findings

The survey shows that OT security maturity remains uneven across critical infrastructure organizations. The findings below capture some of the strongest cross-industry and sector results from the 603-respondent survey.

88% describe their OT security programs as planned or design-led

Only **21%** report a complete asset inventory

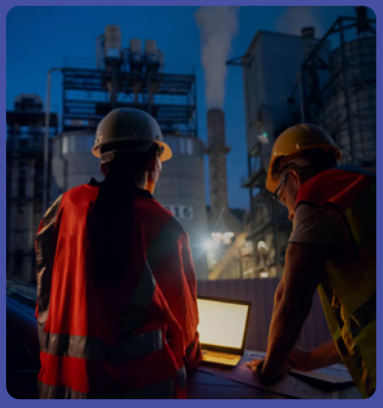
92% place their organizations in the top two tiers of recovery readiness, yet only

31% say they are fully ready

16.2 hours is the **average downtime** reported for respondents' most significant OT cybersecurity incidents

Only **20%** continuously monitor **more than three-quarters** of connected IoT devices such as cameras and thermostats

+17% Among incident-affected respondents, the share reporting downtime of six hours or less is **17 percentage points higher** with stronger asset visibility: 42% vs. 25%



66%

report an audit failure or significant finding during the past year

$100,000+/hr

21% of incident-affected respondents estimate downtime costs above **$100,000 per hour**, including 4% who estimate costs above $500,000 per hour

≥1 day

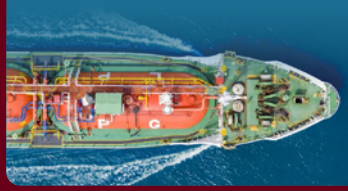
Among incident-affected respondents, the share reporting downtime of at least one day is **9 percentage points higher** for reactive or tool-by-tool programs than for planned or design-led programs: **21% vs. 12%**

+12%

The share expecting restoration within 24 hours is **12 percentage points higher** among organizations passing every audit than among those with audit failures or findings: **87% vs. 75%**

87%

of maritime respondents report a significant OT cybersecurity incident in **the past 12 months**



19%

of healthcare respondents say facility and building systems are fully integrated into cybersecurity monitoring and protection

67%

of healthcare respondents say a significant cyber incident could severely affect caregiver or patient safety or damage physical equipment

91%

of energy and utilities respondents report experiencing a significant OT cybersecurity incident in the past 12 months

28%

of incident-affected oil and gas respondents report effects across multiple regions

Knowing where OT security maturity falls short is only the first step. Honeywell Technologies helps industrial organizations turn benchmark findings into a prioritized cybersecurity strategy that reflects mixed control environments, operational constraints and the systems critical to uptime and safety.

Reach out to assess where your OT security program stands and identify the next steps you can take to strengthen resilience across critical operations.

The threat came through the cooling system

Picture a manufacturing plant whose critical operations depend on an on-site data center. The data center's servers stay online only as long as the chillers keep them cool. Now imagine that the system controlling the chillers sits on a facility network with an unsecured remote access path left open for the maintenance team's convenience.

Shut down the cooling, and the servers fail. Getting a laptop onto the production network may require layers of approval, but an unsecured remote access path can expose a system with the power to disrupt plant operations to someone outside the facility.

Recent attacks on U.S. water utilities show that this kind of OT risk is not hypothetical. By early August 2026, attacks were reported against water systems in at least seven states.[1] The FBI and EPA said attackers had remotely accessed internet-facing programmable logic controllers, causing loss of monitoring or control and, in some cases, degraded water operations.[2] Federal investigators are examining possible links to Iran-backed hackers.

That's the shift in risk industrial organizations now have to measure. OT security increasingly extends beyond traditional production systems. Process controls and field devices now operate alongside connected building, safety and physical security systems that can affect operations, equipment and people.

When these systems are poorly governed or monitored, exposure can extend from a single asset to the entire operation it supports. That makes security coverage a critical maturity question for organizations: Are all connected systems identified, integrated into security operations and actively monitored? Can these critical systems be quickly and safely restored when a disruption occurs?

OT security maturity matters because cyber incidents can affect physical operations and worker safety. They can also disrupt service delivery and create compliance pressure. The high cost of downtime makes maturity a business concern as well.

Our inaugural OT Cybersecurity Benchmark survey, drawn from 603 respondents in critical infrastructure sectors, points to uneven progress in extending OT security strategies beyond traditional production environments.

Where cyber meets physical

OT environments increasingly intersect with systems that control physical processes, support facility operations and protect people and assets. They include:

- Process control systems, field devices and controllers
- Safety systems
- HVAC, chillers, switchgear, elevators and fire panels
- Physical security systems, including access controls, badge readers and CCTV
- Building management systems and connected IoT devices

These systems do more than exchange data. They control physical conditions, equipment and access. A cyber incident can disrupt cooling, halt production, affect patient care or create other safety risks.

Mature OT cybersecurity programs identify these systems, bring them into security scope, monitor and govern them, and prepare to recover them. Clear ownership and access to the right expertise support every step.

Gartner uses cyber-physical systems (CPS) as an umbrella term encompassing OT, industrial control systems and other technologies that interact with the physical world.[3] This report uses OT as its primary term and identifies physical security systems separately where relevant.

Only **16% of respondents** say their organizations continuously monitor more than three-quarters of their building automation systems, and **only 20%** say the same for connected IoT devices such as cameras and thermostats.

These responses indicate that many connected systems remain at least partly outside centralized security visibility. In addition, **35% of respondents** report using manual or procedural controls as part of how they secure third-party access to OT and facility systems.

Taken together, these findings define the OT security maturity model used throughout this report.

Widespread visibility gaps

16%

say their organizations continuously monitor more than three-quarters of their building automation systems

20%

continuously monitor connected IoT devices such as cameras and thermostats

Four capabilities shape maturity

Identifying connected assets

Extending security scope beyond traditional production systems

Monitoring and governing connected environments

Protecting and recovering critical operations

Execution capacity forms the foundation, determining whether organizations can mobilize ownership, expertise, response support and governed automation when disruption occurs.

Sector spotlight

Healthcare

In a hospital, many of the systems that keep care moving sit out of sight. HVAC equipment, access controls, elevators, cameras and building management systems regulate the environment around patients and clinicians. But they may be harder for the security team to see than the medical devices at the bedside.

For example, **44%** of healthcare respondents cite legacy or unsupported medical devices as a significant cybersecurity challenge. They can be difficult to patch or replace without affecting clinical workflows, but they are only one part of a much wider connected environment.

The deeper problem is what remains outside the security team's view. Only **19%** of healthcare respondents say facility and building systems are fully integrated into cybersecurity monitoring and protection. That gap matters because healthcare facilities are part of service delivery. In addition, **67%** say a significant cyber incident could severely affect caregiver or patient safety or damage physical equipment.

A hospital may know that a building system exists and still lack a clear picture of how it's connected, who can access it or what depends on it. Security may see the threat, facilities may understand how the system operates and clinical engineering may know what can safely be changed. During an incident, all of these views must come together quickly.

The survey also points to where healthcare teams have experienced success. Among healthcare respondents whose organizations experienced a security incident, **47%** credit early threat detection with helping them restore operations quickly.

In healthcare, OT security maturity is tested before a crisis. Connected systems and medical devices need to be included in the security program. Clinical, facilities and security teams must also be ready to work together and test response scenarios before disruption affects care.[4]

44%

cite legacy or unsupported medical devices as a significant cybersecurity challenge

47%

credit early threat detection with helping them restore operations quickly

Section 1

OT security must extend beyond production systems

Measuring OT security maturity increasingly requires looking beyond traditional production assets to the safety, facility and physical security systems the program covers.

Many organizations have taken steps to broaden OT security coverage. For example, **64%** of respondents say their organizations **include safety systems**; **57% include physical security systems**; and **56% include facility infrastructure**, a category that can include chillers, switchgear and fire panels.

Yet many organizations still leave connected systems outside the security program. That creates gaps in visibility and protection across the wider operational environment.

The stakes are often physical: **64% of respondents** say a significant incident could have a severe or high impact on physical equipment and worker or customer safety. In operational environments, safety is part of OT security maturity, not a separate concern.

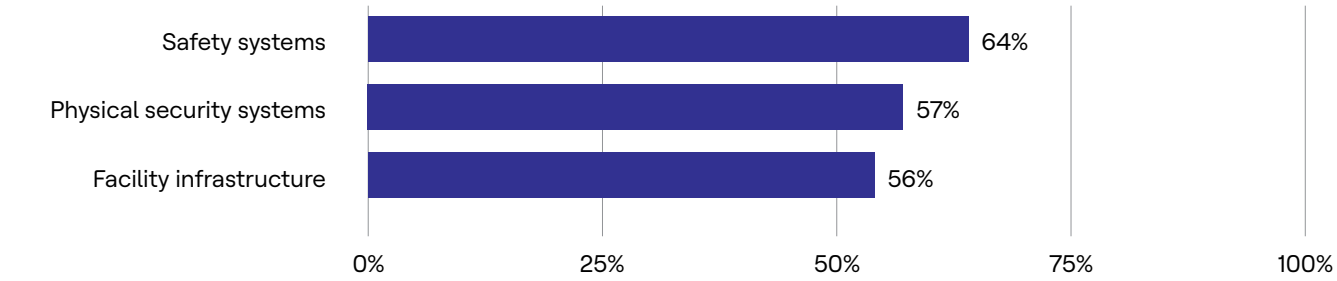
The impact of an incident can extend beyond the initial site. Among respondents whose organizations experienced a significant OT cybersecurity incident in the past 12 months, **40% report that it affected multiple sites in one region** and **16% report effects across regions**. A weakness at one facility can become an enterprise-wide operational risk.

Severe safety impacts

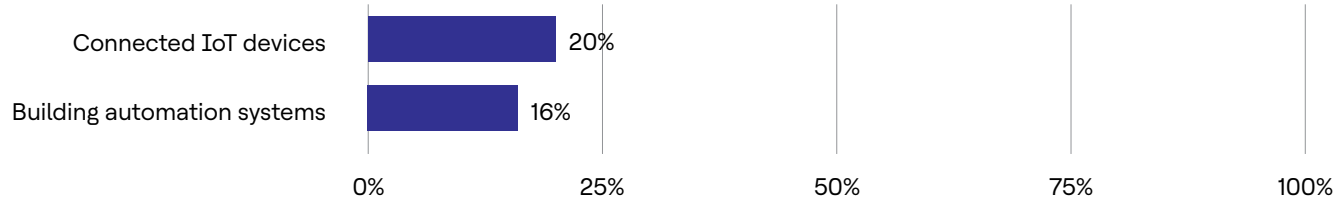
64%

say a significant incident could have a severe or high impact on physical equipment and worker or customer safety

What OT security programs include:



What organizations continuously monitor:



Unplanned downtime makes OT security a board-level concern

When asked about the consequences of cyber incidents, **54% of respondents report operational downtime and production disruption**. That puts the spotlight on recovery speed and effectiveness, which are key measures of an organization's operational resilience.

For their most significant incidents, **respondents report an average of 16.2 hours of downtime**. Among incident-affected organizations, 13% report downtime of at least one day.

The financial impact is also material: 38% report direct financial loss or revenue impact, while 21% estimate downtime costs above $100,000 per hour. For 4%, those costs exceed $500,000 per hour.

OT disruption presents a material business risk. When critical systems go down, production can stop and safety can be compromised. Lost revenue may follow. OT security maturity is ultimately measured by whether organizations understand their attack surface, limit incident impact and restore operations quickly.

Downtime impacts from cyber incidents

54%

report operational downtime and production disruption

38%

report direct financial loss or revenue impact

21%

estimate downtime costs above $100,000 per hour

Incident exposure and expected recovery diverge across sectors

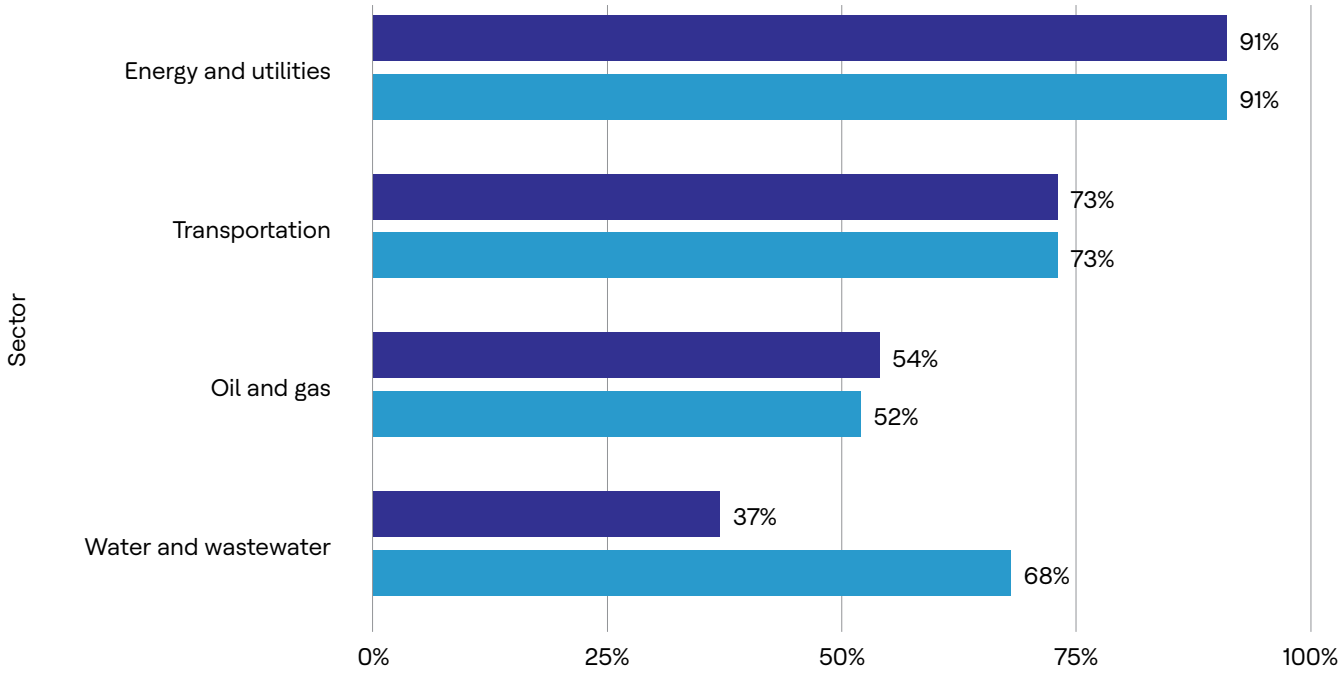
Among the four sectors shown, energy and utilities respondents report the highest incident exposure and the strongest expected 24-hour recovery, at 91% for each. That combination reflects high reported exposure alongside high confidence in the ability to restore operations.

Oil and gas presents a different profile. Although 54% report experiencing a significant incident, only 52% say they could restore critical systems within 24 hours, the lowest expected recovery rate among the four sectors shown.

Water and wastewater respondents report the lowest incident exposure, at **37%,** while **68%** say they could restore critical systems within 24 hours.

Together, these findings show why reported incident exposure alone is an incomplete measure of resilience. What matters is whether an organization can restore critical operations under pressure.

OT incident exposure and expected recovery by sector [5]



Sector spotlight

Energy and utilities, oil and gas

Energy and utilities and oil and gas are both critical infrastructure sectors that supply the energy on which the global economy depends. They are part of the same energy system, but they face different operating realities.

The energy and utilities sector comprises highly regulated, always-on transmission and distribution networks, while oil and gas spans dispersed assets from wellheads and pipelines to offshore platforms.

Energy and utilities respondents report the strongest expected 24-hour recovery result of any sector: 91% say they could restore critical OT systems within 24 hours. The same percentage report experiencing a significant OT cybersecurity incident in the past 12 months, also the highest result in the study.

The oil and gas sector reports a different pattern. In total, **54% report experiencing a significant incident** in the past 12 months, while only **52% say they could restore critical systems within 24 hours**, the lowest expected recovery rate among the four sectors profiled. Among incident-affected respondents, 28% in oil and gas report effects across multiple regions, compared with 10% of affected energy and utilities respondents. In terms of recovery, 28% of oil and gas respondents say they are fully recovery-ready, compared with 36% of energy and utilities respondents.

Both sectors report above-average asset visibility. More than nine out of ten oil and gas respondents, or **91%**, report a complete or mostly complete asset inventory, compared with **85%** of energy and utilities respondents and **80%** across the full sample.

The contrast extends beyond incident exposure. The energy and utilities sector combines high reported exposure with strong recovery confidence. Oil and gas respondents report lower incident exposure, but weaker expected recovery and broader geographic impact among affected respondents. For organizations operating grids, pipelines, wellheads and offshore platforms, resilience depends on turning asset visibility into tested recovery across critical environments.[6]

91%

of energy and utilities respondents say they could restore critical OT systems within 24 hours

54%

of oil and gas sector respondents report experiencing a significant incident in the past 12 months

Section 2

OT security maturity has not reached every layer of operations

Most organizations can point to visible signs of OT security maturity. For example, 88% of respondents describe their OT security programs as planned or design-led, and 80% report strong coordination between IT and OT teams. Yet only **33% say OT is fully integrated** into an enterprise security operations center (SOC) with centralized visibility.

How far visibility extends across the connected systems that keep operations running is a practical test of OT security maturity. Organizations need visibility across operational and facility environments, including physical security systems, and must be able to monitor and restore critical systems when disruption occurs.

OT security program maturity

88%

describe their OT security programs as planned or design-led

33%

say OT is fully integrated into an enterprise security operations center (SOC) with centralized visibility

On these measures, the survey reveals significant OT security maturity gaps. Although **92%** of respondents place their organizations in the top two tiers of recovery readiness, only **31%** say they are fully ready. Another 61% describe themselves as mostly ready, meaning some systems, sites or scenarios have not been fully implemented or tested.

Only **21% report a complete asset inventory**, an essential visibility step for effective monitoring, detection and recovery. That 21% result contrasts sharply with the 88% reporting a planned or design-led security program. An OT security program can be planned, coordinated and well-funded and still miss systems outside traditional production environments. Facility systems, safety systems, physical security systems and connected IoT assets may remain outside its view.

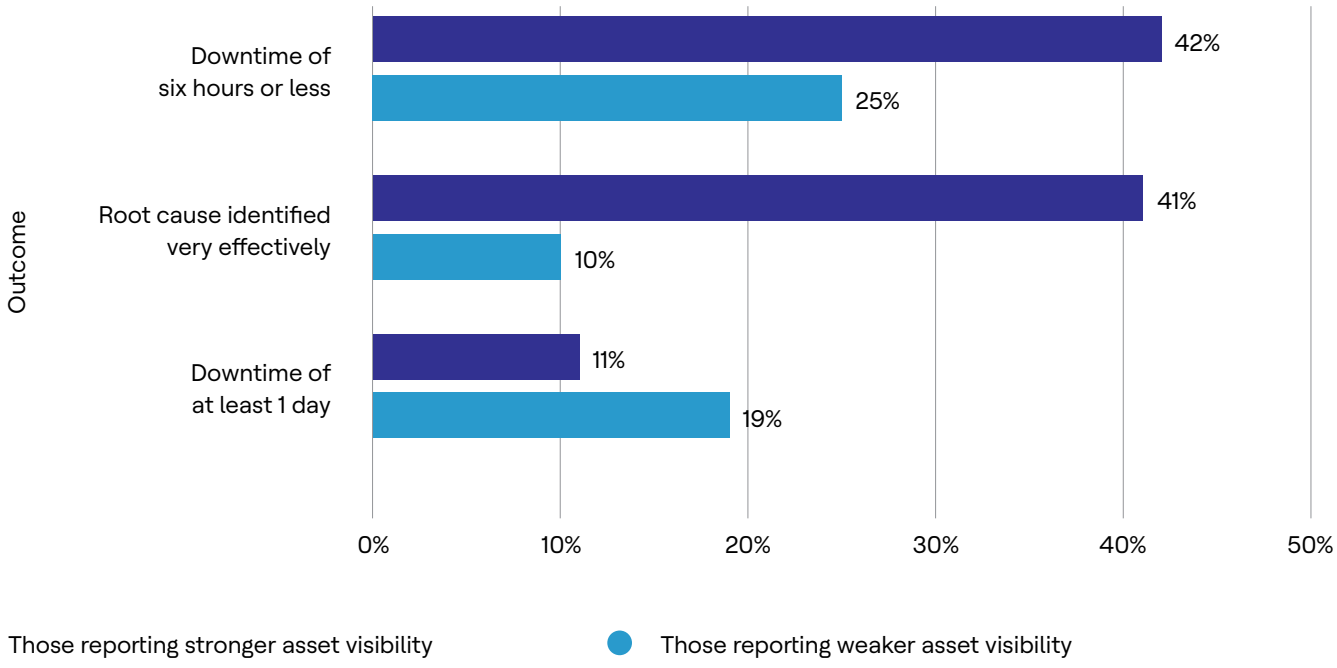
Without that foundation, organizations can't know with confidence whether monitoring, protection and recovery plans extend across every critical system, including those that support production, facilities and safety.

Incident outcomes also vary by asset visibility level, supporting the role of inventory as a core maturity measure. The share reporting downtime of six hours or less was **17 percentage points higher** among respondents with stronger visibility than among those with weaker visibility.

Organizations need continuous visibility across connected systems. They also need to test recovery before disruption puts those plans under pressure.

Stronger asset visibility aligns with faster diagnosis and recovery

Among security incident-affected respondents:



Stronger visibility = comprehensive or substantial inventory; weaker visibility = moderate, limited or no formal inventory. "Don't know" responses excluded. Downtime bases: stronger visibility, n=348; weaker visibility, n=91. Root-cause-identification bases: stronger visibility, n=343; weaker visibility, n=91.

Section 3

Legacy systems remain the common fault line

Legacy systems appear consistently across three measures of OT security risk. Legacy systems and infrastructure constraints rank as the top barrier to better OT security outcomes, cited by 48% of respondents.

Legacy or unsupported systems are also the most-selected source of cyber risk exposure, at 47%. And among incident-affected respondents, 45% rank legacy systems as one of the top three contributors to downtime.

The pattern also appears across sector-specific findings. For **healthcare respondents**, legacy or unsupported medical devices are the top challenge, cited by 44% of respondents. In **maritime**, legacy onboard systems tie with limited onboard security expertise as the most-selected challenges, at 40% each. Among **respondents in oil and gas**, power grid and other energy categories, 45% cite aging or legacy infrastructure.

Legacy infrastructure creates a persistent OT security challenge because industrial equipment is built for long service life. Many machines and devices continue to run critical production and building systems reliably for decades.

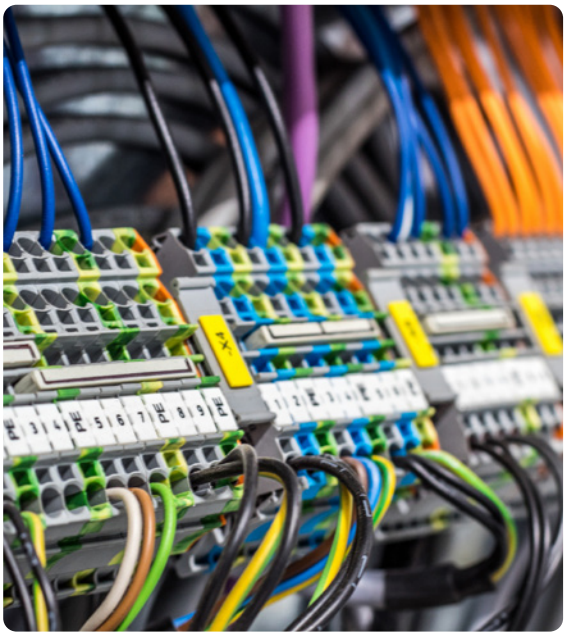
Cybersecurity risk grows when systems designed to operate in isolation become connected to wider networks or are reachable through remote-access pathways. Many legacy controllers run older operating systems and industrial protocols with no authentication or encryption because they were built to operate in isolation.

If an attacker reaches one of these controllers through an IT connection or remote-access pathway, the impact can extend beyond data access. The attacker may be able to change what the controller tells physical equipment to do: trip a breaker, disable a safety interlock, push a setpoint outside a safe range or halt a line. Any of those actions could stop production or damage equipment. Depending on the process, the consequences could also include injury or environmental harm.

That creates a difficult security equation: The systems may be essential to operations but difficult to change without affecting the processes they control. Patching is rarely straightforward. Changes may require extensive validation, planned downtime or vendor support on equipment designed to run continuously. Immediate replacement is often no easier. When patching or replacement is not practical, organizations need compensating controls to manage the exposure while keeping operations safe and available.

That is where legacy systems become a test of OT security maturity. Organizations need to know which aging or unsupported assets are connected across production, building and IoT environments. They also need to understand which operations depend on those assets and what safeguards are in place when patching or replacement cannot happen quickly.

Legacy risk cannot be managed if aging assets are not visible. A complete, continuously updated inventory is the starting point. Segmentation, continuous monitoring and recovery planning help keep those systems from becoming a persistent source of exposure.



Legacy systems and security

48%

rank legacy systems and infrastructure constraints as the top barrier to better OT security outcomes

45%

rank legacy systems as one of the top three contributors to downtime

Section 4

Audit success is associated with stronger recovery readiness

Compliance remains an important part of OT security maturity. Respondents whose organizations passed all compliance audits report significant incidents at nearly the same rate as those whose organizations had audit failures or findings: 74% versus 73%.

That comparison does not show that compliance lacks preventive value. It shows only that audit status did not distinguish reported incident experience in this survey.

Recovery measures show a clearer difference. Among respondents whose organizations passed all audits, **44%** say they are fully recovery-ready, compared with **26%** of those whose organizations had audit failures or findings, an **18 percentage-point difference**.

Organizations passing all audits are also more likely to say they could restore critical OT systems within 24 hours, at 87% versus 75%.

Compliance and recovery readiness

44%

of respondents whose organizations passed all audits say they are fully recovery-ready

26%

of respondents whose organizations had audit failures or findings say they are fully recovery-ready

Only 29% of respondents say their organizations passed all audits with no findings during the past year, while **66%** report an audit failure or significant finding.

Cybersecurity regulations are intended to reduce economic disruption and protect public safety. Organizations that fail to meet required standards may face consequences beyond the audit itself, including fines, remediation costs and potentially higher cyber insurance premiums or more restrictive coverage terms.

The recovery differences may reflect the operational discipline reinforced by compliance programs. Tested backups, documented response procedures and clear ownership can provide audit evidence while also supporting restoration under pressure.

As regulatory mandates expand, governance, risk and compliance (GRC) programs can help organizations translate requirements into operational evidence and tested practices.

For OT security maturity, the important measure is how consistently compliance requirements are translated into tested response and recovery practices.

Compliance and recovery readiness

66%

report an audit failure or significant finding

29%

of respondents say their organizations passed all audits with no findings during the past year

Section 5

Execution capacity shapes recovery from OT disruption

When disruption reaches operational systems, recovery depends on execution. Clear ownership and control-system expertise matter, but so does access to incident-response support that can be activated without creating more operational risk.

No single factor dominates successful restoration. Among incident-affected respondents, 41% credit early threat detection with helping them restore operations quickly, 38% cite resilient recovery capabilities, 34% cite segmented networks and 33% cite autonomous vulnerability mitigation.

Rehearsed response playbooks, clear roles and communication protocols, and rapid original equipment manufacturer (OEM) or control-system vendor support also rank closely together, each cited by 28% to 29% of incident-affected respondents.

Because respondents could select up to three factors, the findings show that fast restoration depends on several capabilities working together. No single control or support resource is enough on its own.

Restoring operations

41%

credit early threat detection with helping them restore operations quickly

38%

cite resilient recovery capabilities

Respondents also see multiple barriers to stronger execution. After legacy constraints, respondents cite concerns about operational disruption at 36%, budget constraints at 33% and **staffing or skills shortages at 32%**. Skills remain a significant constraint, but they are one of several barriers organizations must address.

Program design is also associated with actual downtime. Among incident-affected organizations using reactive or tool-by-tool approaches, **21%** report at least one day of downtime after their most significant incident, compared with **12%** of those using planned or design-led programs.

Execution capacity depends on activating expertise quickly enough to support safe recovery.

That expertise may sit inside the organization or come from OEMs, control-system vendors and managed or co-managed service partners. In mixed environments, support must span technologies and sites.

Barriers to stronger execution

21%

of incident-affected organizations using reactive or tool-by-tool approaches report at least one day of downtime, compared to

12%

of those using planned or design-led programs

Execution capacity concerns

36%

cite concerns about operational disruption

32%

cite staffing or skills shortages

Section 6

AI is already reshaping OT security operations

AI-enabled capabilities are already widely used in OT security operations. AI-enabled threat detection leads at 72%, followed by continuous monitoring at 68% and asset inventory at 59%.

Full autonomy is more unusual. Most AI capabilities still assist human analysts, rather than acting independently. In total, **23% report autonomous or agentic operation for threat detection**, and 23% also report it for continuous monitoring. Separately, 19% report autonomous or agentic operation for asset inventory.

These figures add another dimension to the OT security maturity question: how much authority AI systems are given, how their actions are governed and whether operators can trust them in live production environments.

AI use in OT security

72%

use AI-enabled threat detection capabilities

68%

use AI-enabled continuous monitoring

Asset inventory provides a useful test of AI maturity in OT security. It's the least mature foundational capability among organizations in the survey and has the lowest reported level of autonomous AI use. Among organizations with strong asset visibility, 22% report autonomous inventory capabilities, compared with only 8% of organizations reporting weak visibility.

The data cannot establish whether AI creates stronger visibility or whether organizations with stronger foundations are better positioned to adopt advanced automation. It does show an association: organizations with weaker asset visibility are also less likely to report autonomous asset-inventory capabilities.

In total, **99%** of respondents **expect AI to affect OT security within the next two to three years**. That makes the secure, trusted use of AI an increasingly important measure of maturity. As AI moves from assisting analysts toward taking action, organizations will need clear decision rights, human oversight and testing that accounts for the operational consequences of an incorrect response.

The goal of well-governed AI automation is to strengthen visibility and response without creating new risks to uptime, equipment or safety.

AI and OT visibility

22%

with strong asset visibility report autonomous inventory capabilities, compared with only

8%

of organizations reporting weak visibility

99%

expect AI to affect OT security within the next two to three years

Section 7

What mature OT resilience looks like

OT security maturity starts with visibility. Organizations need a complete, continuously updated view of the systems connected across production, safety, facility and building environments, including physical security systems.

Without that foundation, they can't know whether critical systems are covered by the security program, monitored for threats or included in recovery plans.

From there, maturity depends on four connected capabilities: **identifying connected assets, extending security scope beyond traditional production systems, monitoring and governing connected environments and protecting and recovering critical operations.**

Execution capacity supports all four. Clear ownership, OT expertise and response support determine whether plans can be carried out quickly and safely when disruption occurs.

Incident exposure or audit status alone does not define maturity. Organizations passing every audit report significant incidents at nearly the same rate as those with failures or findings. The clearer test is whether teams can see the full operational environment, coordinate the response and restore critical systems.

AI adds another dimension. AI-enabled detection, monitoring and inventory are already widely reported, while autonomous capabilities remain less common. As autonomous AI capabilities become more prevalent, organizations will need clear decision rights, human oversight and testing that accounts for operational consequences.

Four capabilities shape maturity

Identifying connected assets

Extending security scope beyond traditional production systems

Monitoring and governing connected environments

Protecting and recovering critical operations

Execution capacity forms the foundation, determining whether organizations can mobilize ownership, expertise, response support and governed automation when disruption occurs.

How CISOs can strengthen OT resilience

The findings point to five areas where CISOs and OT security leaders can strengthen maturity:

1. **Maintain a complete, continuously updated inventory of connected systems**. Extend discovery beyond production systems to safety systems, facility and building systems, physical security systems and connected IoT assets. Without continuous visibility, the controls that follow are built on an incomplete picture.

2. **Integrate monitoring across operational environments**. Bring OT visibility together with relevant facility data and signals from physical security systems so analysts can assess both the cyber risk and the potential effects on equipment, safety and uptime before deciding how to respond to an alert.

3. **Manage legacy risk in place**. Identify which aging or unsupported systems remain connected, understand the operations that depend on them and apply appropriate compensating controls where patching or replacement can't happen quickly. Segmentation and continuous monitoring can help reduce exposure.

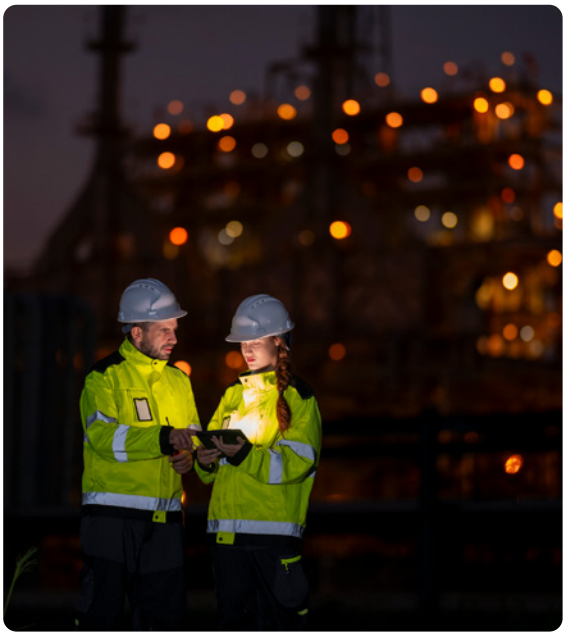
4. **Test incident response and recovery under operational conditions**. Validate whether critical systems can be restored across sites and scenarios. Define ownership before an incident and include operations, engineering, facilities and external response partners in planning and exercises.

5. **Arrange specialized expertise before it's needed**. Ensure control-system knowledge and incident response support can be activated quickly across mixed environments. That capacity may reside internally or come through OEMs, control-system vendors and managed or co-managed service partners.

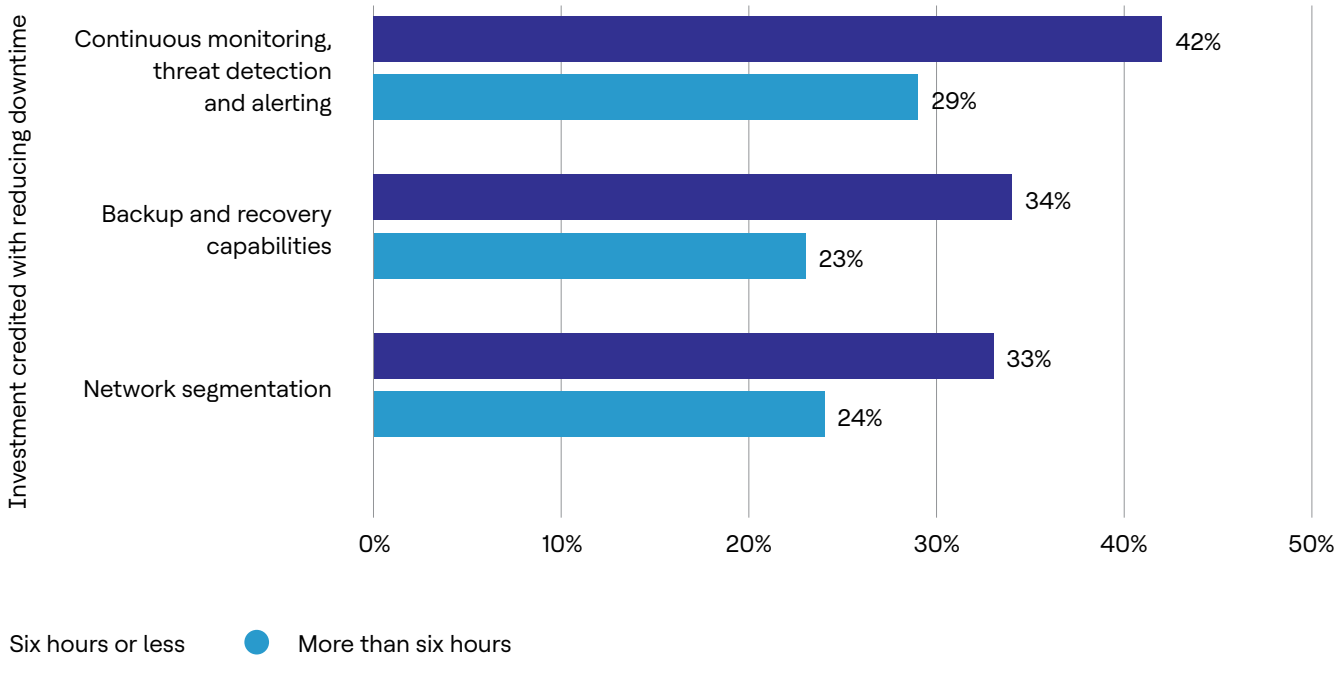
The cooling-system example makes the maturity gap tangible. A system can be essential to uptime and still remain outside the asset inventory, centralized monitoring and recovery plan. Mature OT security programs close those gaps before an incident puts operations at risk.

This benchmark assesses how consistently organizations identify, include, monitor and recover the connected systems that keep operations running. It also examines whether they have the execution capacity to protect people, equipment and uptime when disruption occurs.

The survey's actual downtime results reinforce these priorities. Among incident-affected respondents, organizations with six hours or less of downtime more often credit continuous monitoring, backup and recovery capabilities and network segmentation with reducing downtime than organizations down for more than six hours.



Organizations with shorter downtime tend to credit monitoring, recovery capabilities and segmentation [7]



Sector spotlight

Maritime

Maritime operations place critical OT systems at sea, where response resources may be limited. Vessels and offshore assets may be far from shore. Connectivity can be unreliable. The expertise needed to diagnose or restore a critical system may not be onboard.

The survey reflects those constraints: **40%** cite limited onboard security expertise, **40%** cite legacy onboard systems and **37%** cite intermittent or limited connectivity as top cybersecurity challenges.

This operating reality coincides with a high level of reported OT cybersecurity incidents. Nearly nine out of ten maritime respondents, or **87%**, report a significant OT cybersecurity incident in the past 12 months, compared with **73%** across the full sample.

The potential effects extend beyond downtime: **83%** of maritime respondents say a significant incident could have a severe or high impact on safety or physical equipment, compared with **64%** across the full sample.

Visibility and recovery are where maritime maturity falls short. Only **17%** of respondents describe their organizations as fully recovery-ready, and **47%** report a complete or mostly complete asset inventory, compared with **80%** across the full sample.

For maritime organizations, stronger OT security maturity means being able to see, support and recover the systems that keep vessels, ports and offshore operations moving, even when connectivity is limited and the right expertise is miles away.[8]

17%

of respondents describe their organizations as fully recovery-ready

47%

report a complete or mostly complete asset inventory, compared with 80% across the full sample

Next steps

Turn the benchmark into action

Knowing where OT security maturity falls short is only the first step. Honeywell Technologies helps industrial organizations turn benchmark findings into a prioritized cybersecurity strategy that reflects mixed control environments, operational constraints and the systems critical to uptime and safety.

Our vendor-agnostic OT cybersecurity expertise, global service delivery and managed or co-managed support can help organizations strengthen resilience across complex operational environments.

Reach out to assess where your OT security program stands and identify the next steps you can take to strengthen resilience across critical operations.

[1] Nicole Sganga, "U.S. investigating if Iran was behind cyberattack on water systems in 7 states, including Minnesota and Michigan," updated August 1, 2026.

[2] FBI and U.S. Environmental Protection Agency, "Malicious Cyber Actors Targeting Water and Wastewater Sector Internet-Facing Programmable Logic Controllers, Causing Operational Disruptions," July 30, 2026.

[3] Gartner, "Gartner Predicts That by 2028 Misconfigured AI Will Shut Down National Critical Infrastructure in a G20 Country," February 12, 2026. Gartner defines CPS as an umbrella term encompassing OT, ICS, IACS, IIoT, robots, drones and Industrie 4.0 technologies.

[4] Healthcare base: n=91. Early-detection finding based on incident-affected healthcare respondents, n=59.

[5] Energy and utilities n=66; transportation n=55; oil and gas n=67; water and wastewater n=41. Sector findings should be interpreted directionally.

[6] Energy and utilities base: n=66. Oil and gas base: n=67. Incident-spread figures are based on incident-affected respondents (energy and utilities n=60; oil and gas n=36). Sector findings are directional.

[7] Q34 allowed up to three selections. Base: respondents reporting a significant incident and known actual downtime: six hours or less, n=170; more than six hours, n=269. Findings show an association between investments respondents credit and shorter downtime. They don't establish causation.

[8] Maritime findings are directional because the maritime respondent base is n=30.

Honeywell Technologies is a global automation company serving the building, industrial and process sectors with a broad portfolio of solutions, services and products. Powered by our Accelerator operating system and Honeywell Technologies Forge intelligence platform, the company combines decades of operational data with deep industry expertise from more than 50,000 employees to help customers improve efficiency, resilience and safety while advancing the transition from automation to autonomy.

Honeywell Technologies