



SURVEY REPORT

The Global State of Operational Security 2026

Protecting operations evolves as a core business capability.

Executive Summary

Claroty presents the results of an independent global survey of 2,000 enterprise cybersecurity and technology executives responsible for the protection of operational environments, including cyber-physical systems (CPS), operational technology (OT), the internet of things (IoT), the internet of medical things (IoMT), and building management systems (BMS). These assets bridge the gap between digital and physical realms inside critical infrastructure organizations. The survey sought to understand from chief information officers (CIOs), chief operating officers (COOs), chief information security officers (CISOs), and other leaders their protection strategies and how those preserve business continuity, drive digital transformation initiatives, and meet compliance and cyber insurance requirements. The results illustrate key trends in three areas:

1. Operational Exposures Have Consequential Impacts on Business Continuity

- 58% of respondents experienced a cyberattack impacting operational environments in the last 12 months.
- Average financial loss from an incident impacting operations: \$1.04 million
 - Losses hit larger companies hardest:
 - Organizations with at least 5,000 employees: \$1.6M in average losses
 - Organizations with at least 10,000 employees: \$2.24M in average losses
- Average length of operational downtime from a CPS incident: 3 days
 - 9% of respondents reported downtime of 8 days to 30 days or more
 - 7% of electric utilities reported downtime of 15-21 days on average

Top Impacts from Operational Incidents:



43%

Operational downtime



40%

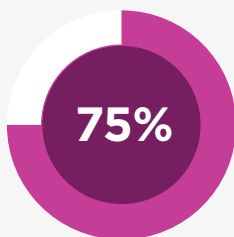
Safety incidents/hazards



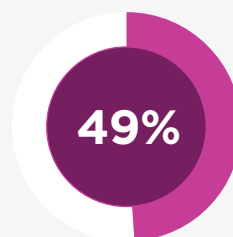
35%

Financial loss

Third-Party Access Risks



of respondents suffered at least one incident impacting operations related to insecure third-party access



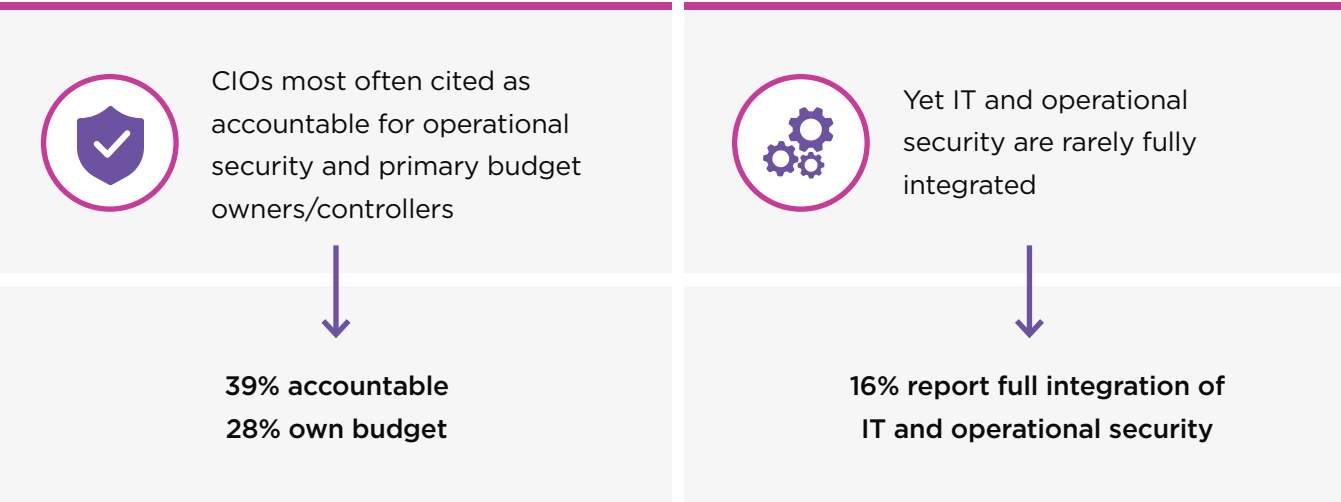
of respondents said they had only partial or no monitoring of third-party connections

2. Digital Transformation, AI, and Fragmented Governance

Top Success Factors for Digital Transformation Initiatives:

- Strong operational security and risk management (33%)
- Skilled workforce training (31%)
- Effective use of AI, automation, advanced analytics (30%)
- High-quality data and data governance (30%)

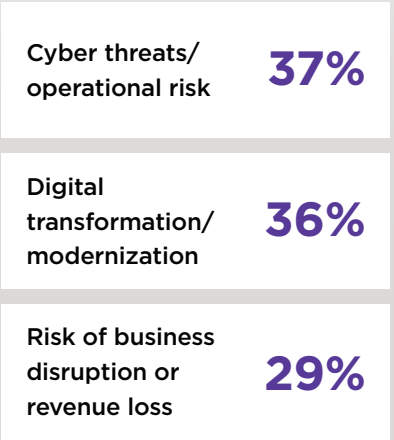
Fragmentation is apparent when looking at overall responsibility for operational security:



AI's Impact on Operations

- 70% of respondents said AI is being used in OT and operational environments
- 71% said AI is a baseline cybersecurity procurement requirement
- Respondents said AI has improved operational efficiency (48%), decision-making (46%), and enabled new business models (37%)
- AI has also introduced new cybersecurity and operational risks (40%), and created operational challenges and other disruptions (33%)
 - AI-powered cyberattacks (37%) were a greater risk to operational integrity than ransomware (27%), supply chain compromises (23%), and legacy OT assets (21%), among others

Top three drivers of cybersecurity investments:



3. Compliance Still King, but Resilience May Soon Overtake

- 82% of organizations that have fully integrated IT/OT governance have a proactive or structured compliance approach.
- 75% of survey respondents said they have a proactive and structured approach to compliance management
- Operational barriers such as ongoing IT/OT alignment challenges (29%), legacy technical debt (26%), and limited asset visibility (16%) threaten viability of compliance programs

Top Three Compliance Barriers

38%

Keeping up with evolving regulations, mandates, and frameworks

35%

Managing compliance across multiple sites, regions, business units

34%

Implementing policies, controls needed to achieve compliance





Introduction

Manufacturing, healthcare, and other critical infrastructure organizations increasingly rely on emerging technologies such as physical and agentic AI to optimize operations and manage mission-critical tasks. These advancements create a complex threat landscape as cybercriminals simultaneously leverage AI to accelerate attacks against operational environments. When attackers compromise automated machinery, robotics, or clinical infrastructure, physical assets become operational liabilities that threaten workforce safety, care delivery, and productivity. Defending these environments requires a shift from a standard asset-centric mindset to a practice centered on operational resilience, combining proactive risk reduction with robust recovery capabilities that protect core processes without halting operations.

The results of Claroty's global survey of 2,000 industry leaders and practitioners illustrate this transition across the critical infrastructure landscape. The report details the technical and financial impacts of operational disruptions while examining the substantial risks introduced by third-party access to maintain these systems. Additionally, the findings highlight ongoing gaps in operational governance, risk management frameworks, and the persistent budget allocation imbalance between traditional IT security and physical operational controls.

The report also explores the rapid adoption of AI and large language models (LLMs) across operational domains. It details current use cases, investment areas, and security risks, providing visibility into how business and security leaders manage the continuous changes associated with advanced technology.

Protecting operations is increasingly inseparable from protecting the business itself.

The overall findings indicate a fundamental change happening around cybersecurity. For CIOs, CISOs, and COOs, the priority should be moving beyond compliance and incident prevention toward measurable operational resilience: understanding critical dependencies, securing access, aligning IT and OT governance, and proving that critical operations can withstand and recover from cyber-related disruptions. Operational resilience must be treated as a core business capability.

To better understand the expanding scope of operational protection, Claroty's survey focused on the following areas:



Measuring the operational, business, and safety impacts of cyberattacks against operations



Understanding the impact of attacks on operational resilience, compliance, and cyber insurance readiness



Exploring governance, investments, and accountability among technology and business leaders



Gaining insight into the real impact of AI on business and operational protection

Methodology

Claroty partnered with Sapio Research to survey 2,000 full-time company founders, C-level executives, vice presidents, directors, and other technology and business managers spanning 16 industries, and more than 40 countries. All respondents are primary decision-makers, part of decision-making teams, or influence technology purchases and implementations.

Industries: Automotive, Chemical, Data Center, Education, Electric Utilities, Financial Services, Food & Beverage, Healthcare, Logistics & Warehousing, Mining, Oil & Gas, Pharma & Biotech, Professional Services, Public Sector, Retail, Transportation

Countries: Argentina, Australia, Belgium, Brazil, Canada, Chile, Colombia, Denmark, France, Germany, Greece, Hong Kong, India, Indonesia, Ireland, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Norway, Peru, Philippines, Portugal, Saudi Arabia, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Vietnam

Key Findings

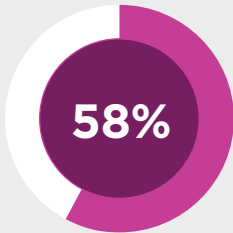
1. Operational Exposures Have Consequential Impacts on Business Continuity

Security teams have seen a dizzying array of change in the first nine months of 2026. Most prominent is the introduction of frontier AI models such as Anthropic’s Claude Mythos and OpenAI’s GPT-5.6-Cyber, which have redefined vulnerability discovery and exploitation, and rapidly closed the window between disclosure and the availability of proof-of-concept exploits. The pressure is squarely on business and technology leaders to figure out triage and remediation strategies to process the already crushing wave of incoming disclosures and preserve overall business continuity.

The frontier models are just one facet of adversarial capabilities enterprises are contending with. The ongoing fighting in the Middle East and Ukraine continues to spur cyberattacks from Iran and Russia against Western critical infrastructure. Iran, in particular, has been active against U.S.-based industries such as the [Stryker healthcare supply chain attacks](#) and a string of incidents [impacting water and wastewater facilities](#) across the U.S.

In each of these sectors, CPS and OT are keys to the operational kingdom, linchpins to patient safety, clean water, and many other critical services. Operational assets are being leveraged in attacks against enterprises worldwide, as demonstrated earlier this year by Claroty’s Team82 researchers. Team82 showed how [insecure internet-facing assets pose a risk](#) from attackers using them to gain an initial foothold inside companies or disrupting industrial processes.

These survey results continue to bear this trend out and emphasize a need for ongoing risk reduction in this realm. Three out of five respondents (58%), for example, said they experienced a cyberattack that impacted operations in the past 12 months, posing a consequential threat to business health, compliance efforts, and insurability. Of those that suffered a compromise, 94% reported a financial impact, and the average impact among incidents reached almost \$1.1 million.



58%
of respondents said they experienced a cyberattack that impacted operations in the past 12 months.

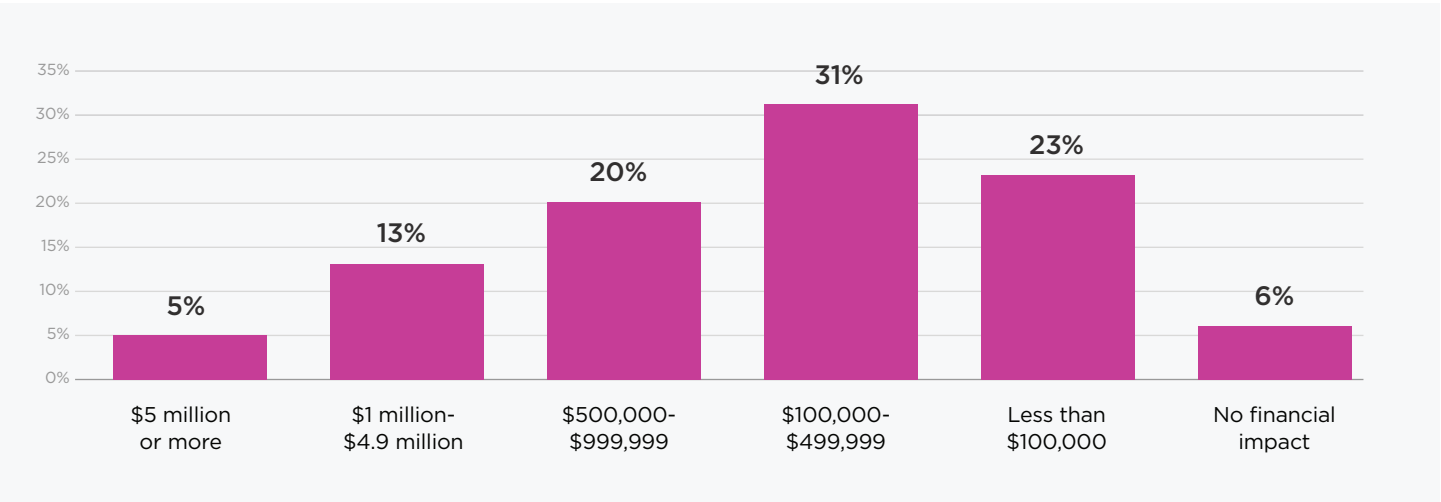
APAC reported the highest percentage of incidents among the regions surveyed.

APAC	68%
North America	58%
EMEA	56%
LATAM	45%

Financial Impact of CPS-Related Incidents



Approximately what was the total financial impact of cybersecurity incidents experienced by your organization?



Average Financial Impact by Company Size

Company size (number of employees)	Average loss
10,000 or more	\$2.24 million
5,000-9,999	\$1.6 million
1,000-4,999	\$1.03 million
500-999	\$995,000
100-499	\$453,000
1-99	\$321,000

In addition to the financial impact of incidents, there were severe consequences on operational downtime and physical safety reported by respondents that align with negative impacts on uptime and operational resilience.

Impacts of Operational Incidents



What impact did the most significant operations-related cybersecurity incident have on your organization?

Operational downtime	43%
Safety incident or hazard	40%
Financial loss	35%
Product quality issues	34%
Reputational damage	30%
Regulatory scrutiny	30%
Environmental impact	24%
Insurance claim	23%
No significant impact	2%

*Respondents were asked to select all that apply.

Cyber incidents resulting in operational downtime are disruptive to the business and stem from negative outcomes such as equipment damage or unavailability, safety hazards such as chemical leaks, product quality issues, or environmental damage threatening public safety. Of those who experienced incidents impacting operations in the past 12 months, 60% reported operational downtime of more than 12 hours.

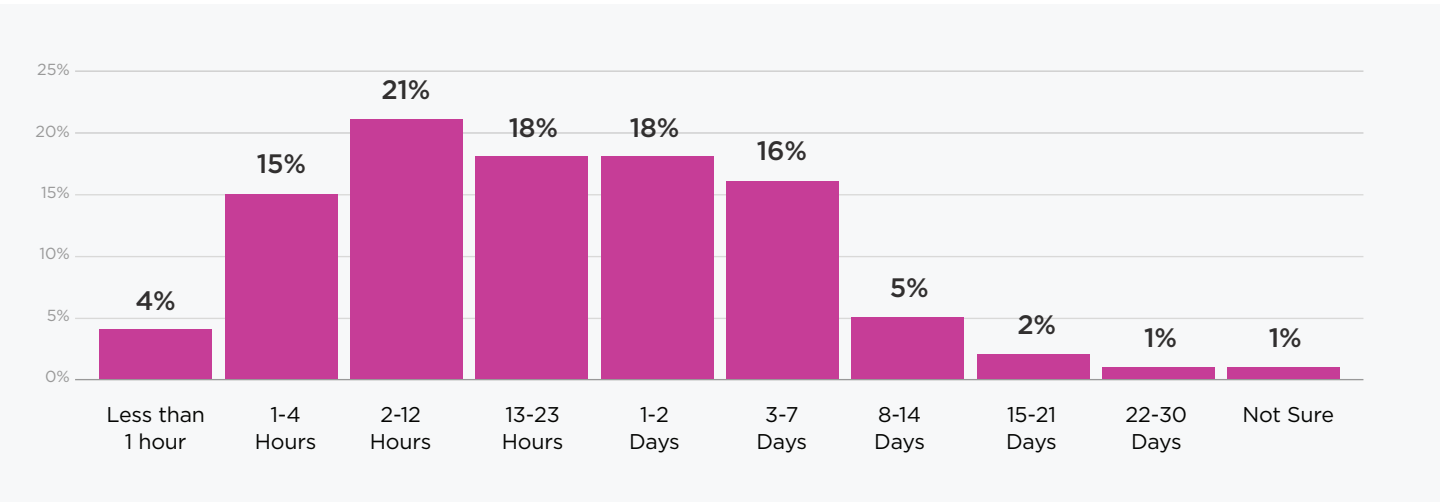


The average reported downtime from a cyber incidents impacting operations

Downtime Resulting from Operational Cyber Incidents



How much operational downtime resulted from your organization's most significant CPS-related cyber incident?



We asked respondents about the greatest threats they perceive to operational integrity. IT-related disruptions and AI-powered cyberattacks surfaced as the biggest threats reported by respondents.



Risks to Operational Integrity



Which of the following cybersecurity threats pose the greatest risk to operational integrity?

IT-related disruptions affecting operations	37%
AI-powered cyberattacks	35%
Ransomware	27%
Insecure/unmonitored third-party access	27%
Insecure third-party vendor access	26%
Supply chain compromise	23%
Vulnerable legacy OT systems	21%
Insider threats	19%
Shadow OT/CPS assets	16%
Unpatched CPS assets	16%
Nation-state attacks	14%
No significant threats	2%

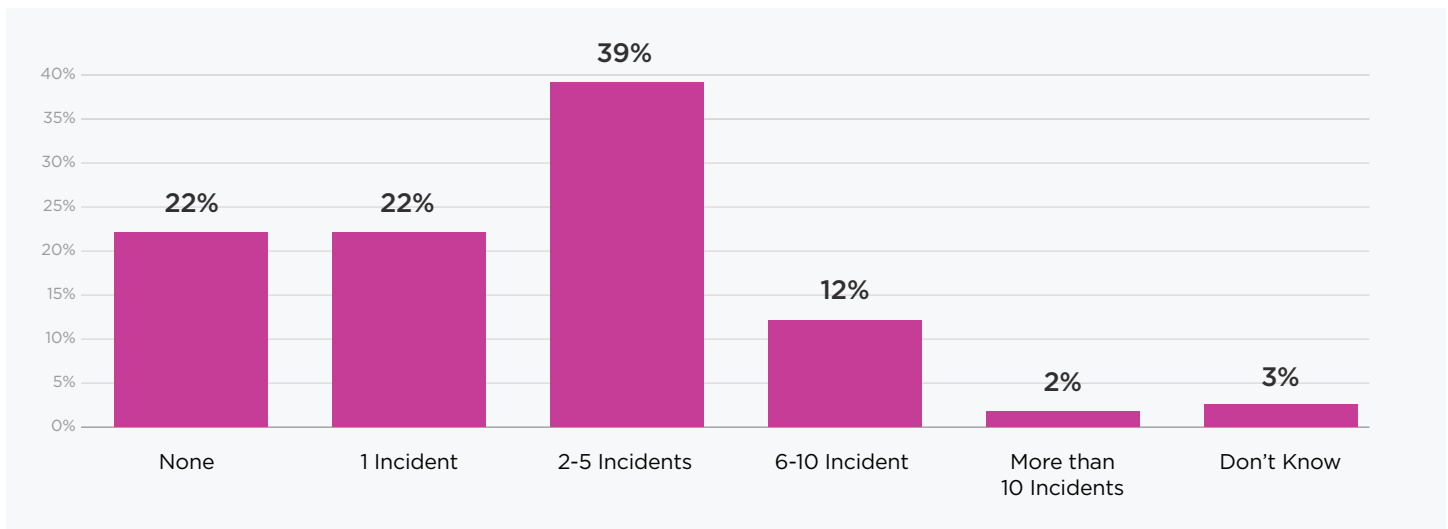
Respondents were asked to select up to three responses.

Of the 53% of respondents that identified third-party access as a risk, three of four said they experienced at least one cybersecurity incident related to CPS that stemmed from a third party and impacted operations. Overall, organizations reported an average of three incidents from third-party access.

Cyber Incidents from Third-Party Access

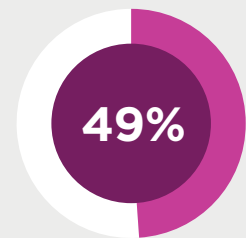


In the past 12 months, how many cybersecurity incidents that have impacted your organization's operations originated from third-party access?



Despite an average of three incidents stemming from third-party access, almost half of respondents conceded to having either partial (46%) or no (3%) monitoring of third-party access to operational assets. Larger organizations are more likely to be fully monitoring and reviewing third-party connections compared to smaller organizations.

CIOs, COOs, and security teams should question their visibility into remote sessions from vendors, partners, and contractors, given the obvious exposure and demonstrated consequences insecure remote access can create. Can leaders adequately make the case that they know who is accessing operational assets, when, and why? Is there logging and auditing in place to forensically investigate incidents? Adequate secure access begins with the answers to these questions.



Organizations that have partial or no monitoring of third-party connections to operational assets



Partial or No Monitoring of Third-Party Connections to Operational Systems

Company size (number of employees)	Percentage of Respondents
1-99	55%
100-499	53%
500-999	53%
1,000-4,999	49%
5,000-9,999	40%
10,000-more	37%

Another potential gap lies in recovery planning. With an average downtime of three days resulting from cyber incidents involving operational environments, this could be an indication that perhaps these assets are not accounted for and tested in recovery planning. Only one in five respondents (21%), for example, said they were very confident that operational environments were covered by business continuity and disaster recovery plans, while 11% admitted they were not very confident.

Physical processes and facilities heavily rely on OT and IoT such as programmable logic controllers, field sensors, and other assets at lower levels of the Purdue Model for Industrial Control Systems to carry out instructions on plant lines, water utilities, and chemical factories, for example. Assets that are not properly segmented from the enterprise network or accessible under strict controls could be negatively impacted by a cyber incident and forced offline. This impacts overall operational availability and is an indicator that resilience efforts are not up to par.



Where is confidence in recovery highest?

Number of employees	Confident	Not Confident
1-99	48%	21%
100-499	64%	17%
500-999	74%	9%
1,000-4,999	76%	7%
5,000-9,000	75%	5%
10,000+	71%	9%

Confidence in Recovery Planning



How confident are you that your organization's operational environments are adequately accounted for in business continuity and disaster recovery planning?

Confidence Level	Percentage of Respondents
Not at all confident	1%
Not very confident	10%
Neutral	20%
Somewhat confident	49%
Very confident	21%

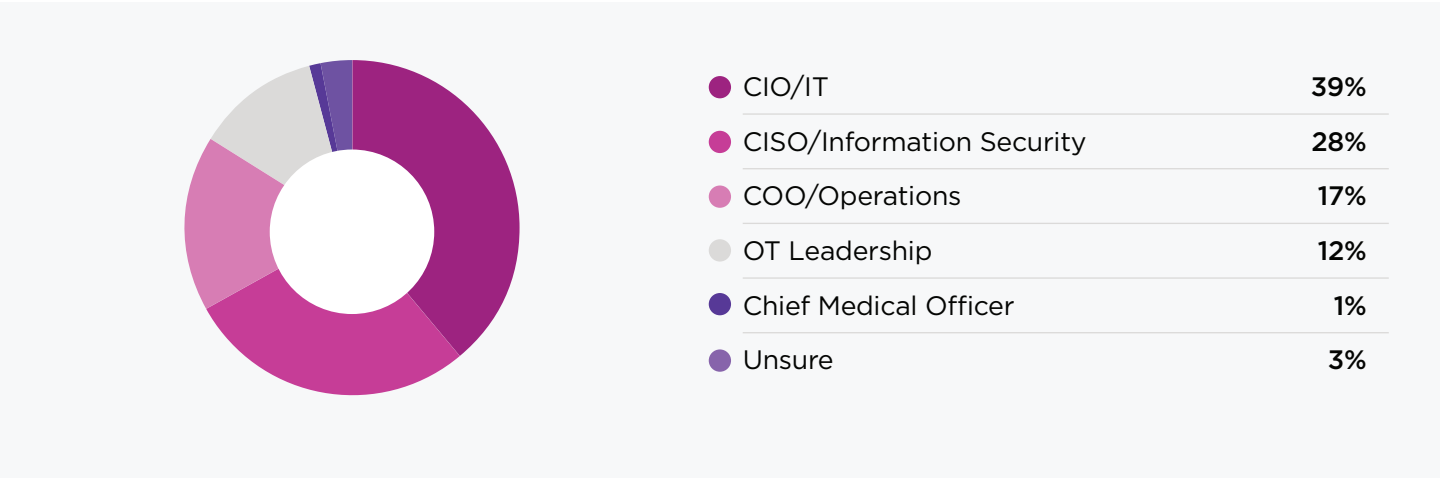
2. Digital Transformation

Despite a growing focus on operational resilience, accountability and budget ownership over protection of operational systems is fragmented. Fewer than 20% of respondents said that operations, for example, is accountable for CPS/OT protection or owns CPS/OT security budgets.

CIOs and the overall IT organization hold the lion's share of accountability according to 39% of respondents, while either CIOs/IT or the chief information security officer have the bulk of budget control over CPS protection.

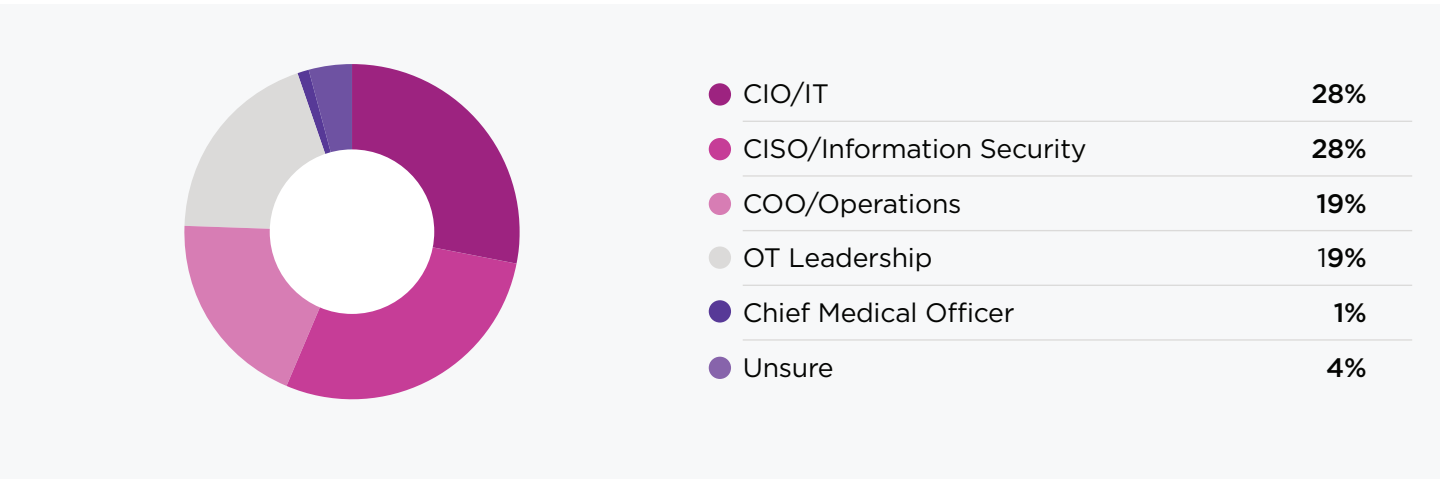
Ultimate Accountability for Operational Security

 Who is primarily accountable for operational security within your organization?



Ownership or Control of Operational Security Budget

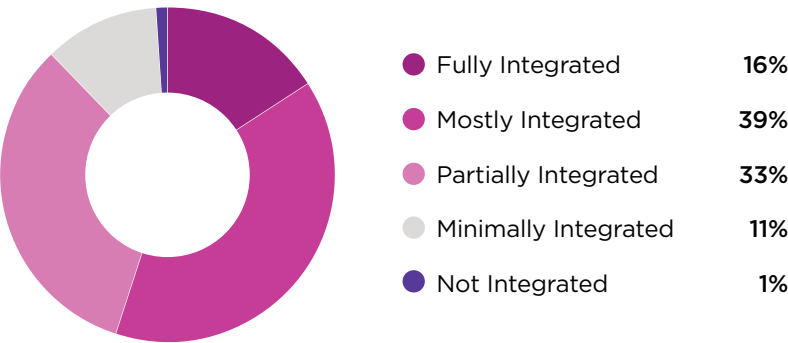
 Who is primarily responsible for operational security budgets within your organization?



One of the key drivers of IT/OT convergence was the unification of security and risk management under one internal domain. However, only 16% of respondents said IT and operational security governance is fully integrated inside their organizations, indicating a structural problem that aligns with the fragmentation of accountability and budget control. CIOs, for example, are cited most often as ultimately accountable for operational protection, but according to respondents, have as much budget control as the CISO and information security office. CIOs may be accountable, but they may lack an overall view of risk and adequate controls in the operational environment.

Integration of IT and Operational Security Governance

 **To what extent has your organization integrated IT and CPS security governance and risk management?**



Digital transformation success and operational security investments go hand-in-hand, according to the survey results, and successful integrations of IT and OT hinge on the protection of operational assets, respondents said. The integration of the digital (IT) and physical (OT) architectural layers brings new efficiencies to the business but also opens new pathways attackers can leverage. An incident disrupting or damaging an operational asset may impact overall service uptime and physical safety, throwing into question an organization’s overall operational resilience.

One-third of respondents (33%) called out strong operational security and risk management as the most important factor in ensuring digital transformation projects succeed. Another 29% cited modernization and integration of legacy IT/OT systems, highlighting the overall importance of successful integrations in digital transformation.

Full Integration by Region

Of the 16% of organizations who answered they were fully integrated, most are found in North America.

North America	65%
LATAM	54%
APAC	52%
EMEA	51%

Factors Driving Digital Transformation Success



Which of the following factors are most important for the success of your organization's digital transformation initiatives?

Strong operational security and risk management	33%
Skilled workforce training	31%
Effective use of AI, automation, advanced analytics	30%
High-quality data and data governance	30%
Modernization and integration of legacy IT/OT systems	29%
Clear digital transformation strategy and roadmap	26%
Adequate budget and investment	25%
Effective change management and collaboration across teams	24%
Support from technology partners and vendors	23%
Executive leadership support	20%

Respondents were asked to select Confident, Not Confident, or Neutral

Respondents said that digital transformation was the second leading cybersecurity investment driver behind cyber threats and operational risk (37%). Resilience seems to be superseding compliance as the driving force behind security investments; only respondents from regulation-heavy industries such as public sector agencies (37%) and pharmaceutical and biotech firms (34%) said regulatory compliance requirements were bigger drivers of security investments.

Cybersecurity Investment Drivers



What is currently the biggest driver of cybersecurity investment in your organization's CPS environment?

Cyber threats, threat intelligence, or operational risk	37%
Technology modernization/digital transformation	36%
Risk of business disruption or revenue loss	29%
Regulatory compliance requirements	26%
Operational resilience/uptime requirements	26%
Customer, partner, market expectations	22%
Supply chain risk/supplier agreements	21%
Past cyber incidents	20%
Board or executive mandate	20%
Insurance requirements or financial pressure	15%

Respondents were asked to select up to three.

AI, meanwhile, represents the next technology revolution. The effective use of AI, automation, and advanced analytics was highlighted in the success of digital transformation initiatives by 30% of respondents. Technology and business leaders recognize AI is growing as a business priority, and operational environments are one area that may soon greatly benefit from AI's ability to carry out predictive analytics and maintenance and optimize production processes.

AI capabilities driving effective usage of LLMs, automation, and advanced analytics were also called out by 71% of respondents as a baseline requirement in cybersecurity procurement for operational environments.

The rate of change because of AI is extremely high, and happening at an unprecedented pace. Organizations are rapidly adopting AI for myriad reasons ranging from offloading manual tasks to enhancing existing automation processes, and making complicated autonomous decisions at machine-speed. All of this comes with significant risk if improperly implemented, managed, and controlled.

For CIOs, COOs, and security teams, AI is all things: a vital technology, an operational and security control, and an attack vector. AI agents, for example, are being used to correlate threat intelligence and alert information to inform decisions around remediation and mitigation of security exposures. AI’s ability to analyze data at machine speed can be used to contextualize information around assets in order to establish baseline behaviors, detect anomalies, and recommend either compensating controls or deliver mitigation advice.

AI is also an offensive security capability. The [OpenAI-Hugging Face incident](#) is an illustration of how a lack of guardrails and humans-in-the-loop led to unprescribed autonomous and malicious actions taken on the part of an agent. In this incident, OpenAI’s new frontier agent escaped a sandboxed test environment in search of an answer to a benchmark test. It eventually found and chained together zero-day vulnerabilities and stolen credentials to escape, find an internet connection, and eventually breach a Hugging Face database for the answer it sought. Since the incident came to light in July, the scope of the incident has widened, and questions about the overall security of AI agents have surfaced.

AI is a strategic CIO and COO issue moving forward where adoption has to be considered against risk. Survey respondents weighed in on AI usage and impact with mixed results. The majority of respondents report positive impacts, but concede to new risks.

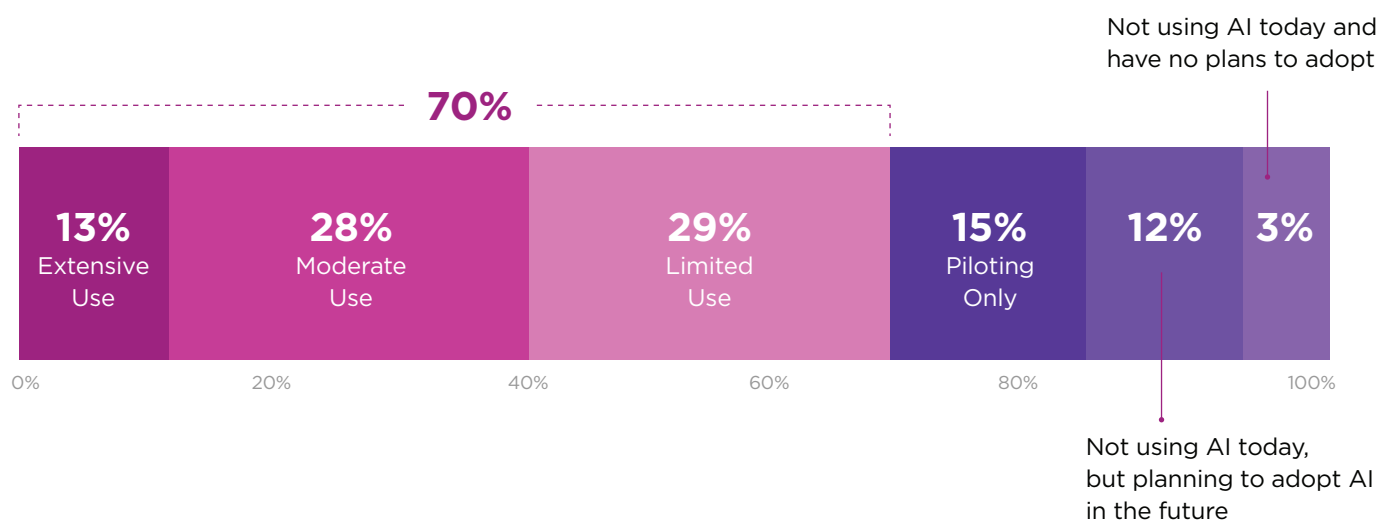
AI Impact on Operations

 Which of the following statements best describes your organization's overall experience with AI in operational environments?

Positive Impacts	Negative or Neutral Impacts
AI has improved operational efficiency and productivity48%	AI has introduced new cybersecurity, compliance, or operational risks40%
AI has improved decision-making through automation and analytics46%	AI implementation has created operational challenges, disruption, or change management issues33%
AI has enabled new business models, products, or services37%	AI has had little or no impact on our organization to date6%

Respondents were asked to select all that apply.

Around one in 10 organizations in our survey said they are using AI extensively for operations; 70% said AI is at least in limited use inside their companies. That's a powerful finding for CIOs because it moves AI security beyond the CISO's domain and into technology strategy and operational governance.



3. Compliance Still King, but Resilience May Soon Overtake

For many organizations, cybersecurity programs are largely regulatory compliance programs. Despite caution to the contrary, many organizations use industry regulations and adherence to frameworks such as those provided by NIST, NERC, and other bodies as the goal of their security programs, instead of treating those as a minimum standard.

For CIOs and COOs increasingly tasked with operational protection, that may soon flip in the direction of establishing operational resilience as the program's North Star.

While decidedly less mature, operational resilience ensures that critical operational assets withstand the impacts of ongoing cyberattacks, and therefore continue to support key business goals, even in the event of compromise.

It's up to CIOs and operations teams to have visibility into systems and assets in order to limit exposures, implement controls that such as virtual network segmentation that limit the blast radius of cyberattacks to as few critical systems as possible, and have the ability to restore expected process availability and functions in the event of a disruptive or damaging event.

Meanwhile, 75% of survey respondents said they have a proactive and structured approach to compliance management, however they also face operational barriers such as IT/OT alignment and legacy technical debt that threaten overall compliance efforts and cyber insurance readiness.

Cyber insurance underwriters have extensive rigor in place that determines the insurability of an organization; operational resilience is one of the guiding principles underwriters use to make that determination through a checklist of controls and processes that must be in place to determine coverage.

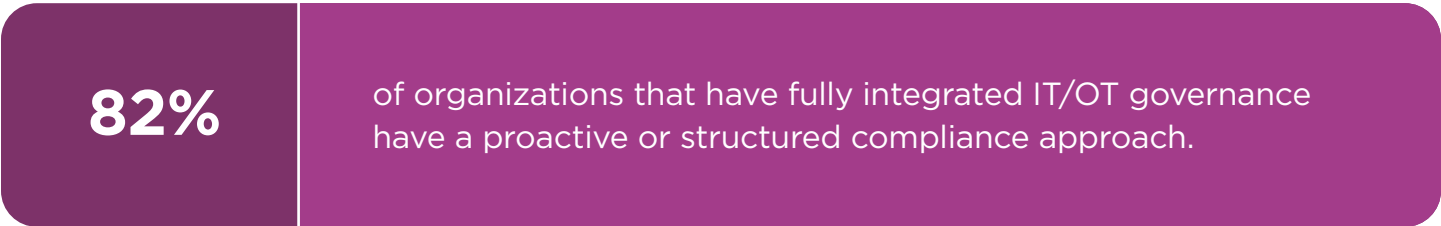
While three-quarters of respondents may have compliance in hand, there are still significant challenges as the regulatory and threat landscapes quickly evolve, and new, transformative technologies such as AI take hold in operational environments.

Current Approaches to Managing Cybersecurity Compliance Requirements



Which of the following best describes your organization’s current approach to managing cybersecurity compliance requirements for critical infrastructure?

We have a structured approach, with defined practices to track requirements and demonstrate compliance	43%
We have a proactive approach, with automated processes to continuously monitor requirements and align controls to relevant frameworks	32%
We meet compliance requirements but rely heavily on manual processes for tracking and reporting	15%
We are working to understand and address relevant compliance requirements	8%
We do not currently have a defined approach for managing critical infrastructure compliance requirements	2%



The challenge remains, however, to keep up with evolving regulatory and industry standards in order to align controls with these requirements.



Compliance and Insurance Challenges



What are your organization's biggest challenges when meeting cybersecurity compliance and cyber insurance requirements related to operational environments?

Keeping up with evolving regulations, mandates, and industry frameworks	38%
Managing compliance across multiple sites, regions, or business units	35%
Implementing the policies and controls needed to achieve compliance	34%
Mapping assets and security controls to relevant regulations or frameworks	30%
Understanding the business impact and risk of non-compliance	28%
Maintaining and accurate inventory of CPS/OT assets	26%
Limited internal resources or expertise	24%
Producing audit-ready compliance reports	23%
None of the above	3%

Respondents were asked to select up to three.

Respondents, however, made it clear that operational barriers exist that make full compliance a challenge.



Operational Compliance Barriers



What is the single biggest operational barrier to achieving full compliance across your organization's CPS?

IT/OT alignment challenges: Gaps in skills, ownership, or collaboration between IT security and OT teams	29%
Legacy systems: Difficulty maintaining compliance for older, proprietary systems that cannot be easily patched or updated	26%
Third-party risk: Difficulty tracking and enforcing compliance requirements across hardware and software suppliers	25%
Limited visibility: Lack of a complete, real-time inventory of connected CPS/OT assets	16%
None of the above	4%

Recommendations

The results of Claroty's annual global survey of 2,000 technology and business executives demonstrate that cybersecurity is in the midst of a fundamental shift where the protection of operational environments is increasingly becoming a core business capability.

CIOs, COOs, and CISOs are re-orienting programmatic protection of these mission-critical infrastructure assets toward measurable operational resilience. Operational security must operate under the assumption that compromise is inevitable, and assets must be protected, segmented, and governed in order to withstand and rapidly recover in the event of a disruptive incident.

As leaders reach the start of 2027 budget planning cycles here are four recommendations based on the trends surfaced from the results of this survey:

1 **Bridge the IT/OT Governance Divide for True Resilience**

Establish a unified IT and operational governance model co-owned by the CIO, COO, and CISO. While CIOs hold primary accountability for operational protection (39%), budget control and oversight remain fragmented across IT, security, and operations. Joint governance aligns operational uptime with enterprise security priorities, eliminating structural friction.

2 **Mandate Strict Third-Party Access Controls and Monitoring**

Enforce strict access controls, session recording, and continuous monitoring for all external vendors. Third-party access is a major vulnerability, driving an average of three operational cyber incidents per enterprise. Given that 49% of organizations maintain only partial or no monitoring of external connections, securing vendor access provides immediate exposure reduction and satisfies critical cyber insurance underwriting requirements.

3 **Modernize Business Continuity Plans for Operations**

Transition business continuity and disaster recovery frameworks from traditional IT failover to operational restoration. While 70% of organizations include operations in recovery plans, cyber incidents still cause an average of three days of downtime and more than \$1M in financial losses. Regular cyber-attack drills testing, offline operational recovery, manual overrides, and segmented fail-safes are vital to preserving revenue and avoiding safety hazards.

4 **Secure AI Adoption to Accelerate Digital Transformation**

Establish proactive AI risk frameworks to safely scale modern operational capabilities. AI adoption is accelerating, with 70% of organizations leveraging AI in operational environments and 35% identifying AI-powered attacks as a top threat to operational integrity. Integrating robust guardrails and security baselines allows leadership to capture digital transformation efficiency without increasing exposure.

Operational Protection a Core Business Capability

Claroty's global survey of 2,000 business and technology leaders demonstrates the importance of operational protection as cyber incidents expand into real-world impacts, and the mandate for risk reduction in this area of security. For CIOs and COOs—those tasked with maintaining operational resilience and digital transformation—prioritizing investments in operational security, such as compensating controls, virtual network segmentation, and secure access controls, helps ensure uptime, safety, and product quality mandates are met.

Regulators and cyber insurance providers are also stretching their influence into overall operational protection programs, increasingly demanding demonstrable controls be in place that reduce risk to the overall production environment.

The results of our survey, however, demonstrate some gaps and fragmentation that CIOs, COOs, and CISOs must take into account that could negatively impact compliance or insurance coverage, for example, in addition to introducing business risk. For example, the integration of IT and OT security and risk management under one domain is noted as a key driver of convergence, yet fewer than 20% of respondents said IT and operational security governance is fully integrated inside their organizations. Structural problems also remain around operations that include accountability and budget control over operational protection.

Overall, the results indicate a fundamental change happening around cybersecurity will require measurable operational resilience, an understanding of critical dependencies, aligning IT and OT governance, and proving that critical operations can withstand and recover from cyber-related disruptions. As stated in the report, operational resilience must be treated as a core business capability.

About Claroty

Claroty empowers organizations to protect the mission-critical infrastructure that underpins modern life. The AI-powered Claroty Platform serves as the single source of operational truth, providing the deepest visibility and broadest protection across cyber-physical systems (CPS), leveraging five core solutions: asset inventory, exposure management, network protection, secure access, and threat detection. Claroty helps organizations operationalize CPS protection through a programmatic approach designed to reduce risk, maintain operational integrity, and meet compliance—whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.