CLAROTY

The Global State of CPS Security 2025: Navigating Risk in an Uncertain Economic Landscape

Claroty presents the results of a survey of 1,100 cybersecurity professionals and their approach to managing CPS security programs in light of economic uncertainties.

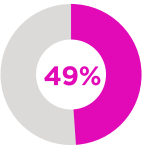
Executive Summary

Claroty presents the results of its annual global survey of 1,100 cybersecurity professionals responsible for the protection of cyber-physical systems (CPS). CPS is at the core of mission-critical infrastructure, including operational technology, connected smart devices and buildings, healthcare delivery organizations, and connected medical devices. In today's fast-changing economic climate, security and business leaders are navigating enhanced CPS risk. The survey sought to understand how the current climate is affecting risk-reduction efforts at the foundation of CPS security programs.

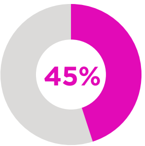
1. CPS Risk Grows in Tandem with Uncertainty

✓ Respondents were consistent in expressing their concerns about the protection of CPS in their environments given unpredictable circumstances in the global economy. Many cited concerns over supply chain disruptions and how existing compliance efforts may be impacted.

✓ In addition to concerns over reducing cyber risk to key assets and gaining a complete understanding of asset exposures, respondents cited a number of other operational impacts from this uncertainty, foremost an inability to meet regulatory mandates or manage risks from third-party access to CPS.



49% of respondents report that supply chain changes caused by shifting global economic policies and geopolitical tensions around the world are leading to increased CPS cybersecurity risk.



45% of respondents are also concerned about their ability to reduce CPS cybersecurity risk, and in their overall understanding of their risk posture.

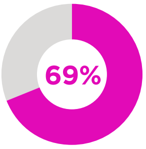
2. Compliance/Regulatory Changes—and a Coming Overhaul?

Organizations with CPS security programs largely standardized on established frameworks such as the NIST Cybersecurity Framework and ENISA in Europe may soon need to build on those frameworks as governments increase regulations.

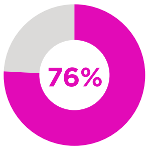
While governments are implementing regulations due to the high risks to critical infrastructure, increasing regulation could disrupt current activities around existing security programs, which are guided at the moment by a blend of industry standard frameworks and government requirements (see chart at right), rather than internal risk assessments, for example.

Top 3 Drivers of Compliance Initiatives

Government Regulations	44%
International Regulations	41%
Industry-Specific Regulations	40%



We see this reflected in the survey results, whereby **69% of respondents** said their current CPS security programs closely adhere to international and local cybersecurity standards or mandates.



However, 76% said emerging regulations may require them to overhaul their current security strategies.

3. Supply Chain Shifts Likely to Increase Already High Third-Party Access Risk as Attackers Will Look to Target the Seams

- **67% of respondents** said they're reconsidering their supply chain geography in order to mitigate the risk of economic and geopolitical uncertainty.
- A ripple effect of shifting supply chains is the escalation of risks associated with third-party remote access, as organizations re-evaluate their vendors and introduce new remote access tools into complex and exposed CPS environments.
- **73% of respondents** are already on this journey, and said third-party remote access to CPS operations is being re-evaluated, with companies demanding visibility into a third party's security posture.
- This may exacerbate existing security challenges involving third-party access to CPS, as **46% of respondents** said they've been breached in the last 12 months because of third-party access and **54%** report they've discovered security gaps or weaknesses in vendor contracts post-incident.

Top 3 Reasons Third-Party Access Is Being Re-Evaluated

Risk Reduction	46%
Cost Savings	38%
Lack of Visibility	33%

Introduction

Intensifying threats and the connectivity that accompanies digital transformation have introduced unprecedented urgency to secure cyber-physical systems (CPS). That urgency to enhance CPS security, however, is countered by economic tensions that expose a lack of confidence around the integrity and availability of the supply chain, and the shadow of consequential regulatory changes on the horizon.

As business and cybersecurity leaders face the prospect of shifting supply chain relationships and compliance overhauls, uncertainty only serves to put CPS and critical infrastructure at greater risk.

Companies are confronting the prospect of long, hard looks at their cybersecurity programs as they balance demands for cyber resilience and business continuity, under the spectre of intensifying threats and shifting regulatory mandates. All the while, risk is on the rise.

This survey aims to describe the current and future state of CPS protection, and illuminate how organizations may be adjusting their cybersecurity strategies in light of economic instability globally.

To understand the current attitudes and approaches toward reducing CPS risk, Claroty's survey focused on several areas:

- How the economic climate is manifesting increased CPS risk
- Whether the uncertainty around trade restrictions is going to narrow the supply chain available to ensure CPS resilience
- Understanding how emerging regulations would drastically change current CPS compliance programs
- Changes to supply chain management, and risk assessments of suppliers and partners in the current climate, and how conditions are affecting risk and threat remediation
- Securing third-party access to CPS and how current high-risk conditions are driving a re-evaluation of remote access

Methodology

Claroty contracted with research firm Pollfish to survey 1,100 full-time information security, OT engineering, clinical or biomedical engineering, and facilities and management or plant operations professionals. Respondents spanned 20 countries across the Americas, Europe, and Asia-Pacific, and more than a dozen industries, including automotive, chemical, food and beverage, healthcare, pharmaceutical and biotechnology, power and energy, transportation, and others.

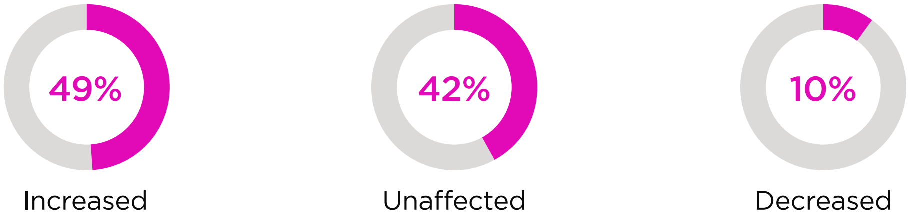
Key Findings

1. CPS Risk Grows in Tandem with Uncertainty

Economic stressors are bringing upheaval to markets and forcing security leadership to re-strategize approaches to CPS security. Respondents cited their concerns over the risk caused by these potential disruptions in many of their responses to our survey.

As they consider how the current economic climate impacts the supply chain and their existing compliance efforts—two major drivers of any security program—they come to a common conclusion with nearly half of respondents reporting that economic impacts on the global technology supply chain are increasing risks within their organizations.

To what extent is your organization's cyber risk affected by supply chain changes caused by shifting global economic policies?



*Percentages may not total 100% due to rounding.

Respondents also expressed concern over perceived operational impacts as a result of the current instability, foremost among them is their ability to reduce cyber risk to key CPS assets and critical processes, or having full visibility into the company's overall risk posture.

Top 10 Operational Impacts*

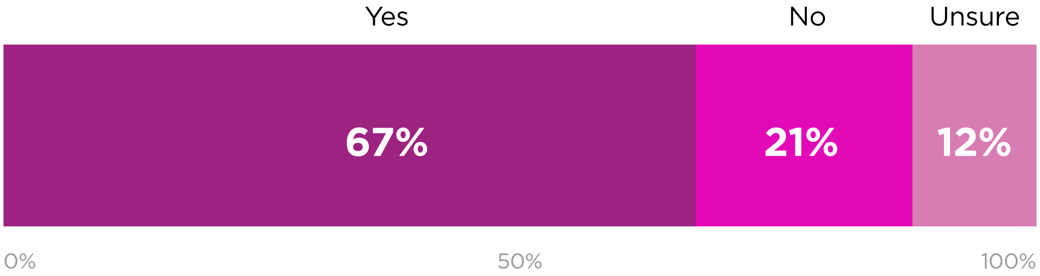
1	Reducing cyber risk to key assets/processes	45%
2	Understanding our risk exposure	44%
3	Meeting industry or national/ regional regulatory mandates	34%
4	Inability to manage the access risk of our third-party suppliers	31%
5	Prolonged exposure to threats	28%
6	Challenges in recruiting and retaining the right talent	27%
7	Having an accurate inventory of our assets	24%
8	Unclear ROI on existing cybersecurity efforts	23%
9	Legacy tech systems lacking security capabilities	18%
10	Interoperability issues among existing solutions	9%

*Respondents were asked to select all that apply.

Threats of future restrictions are also forcing organizations to re-think from where they're sourcing technology. Sanctions and restrictions on key tech industries such as semiconductors and artificial intelligence dating back to the first Trump presidency and the Biden administration, are impacting innovation and competition in numerous geographic markets. Meanwhile, contentious arguments have also been made around national security concerns, intellectual property theft, and perceived trade imbalances with regard to non-domestic suppliers.

Reflecting those ideas, more than two-thirds of respondents say they may be forced to reconsider their supply chain partners as a result of the current climate.

Are you reconsidering your supply chain geography to mitigate cyber-physical systems (OT, IoT, IIoT, IoMT or BMS) security risks or economic unpredictability?



AI’s Role in a CPS Security Strategy

Key components of CPS security programs going forward are artificial intelligence (AI) and machine learning (ML). Organizations are keen to leverage these advanced technologies for a number of crucial capabilities in defending CPS environments.

AI, for example, should figure heavily as a foundational risk-reduction strategy going forward, especially as CPS security programs mature. Organizations can leverage its capabilities to improve threat detection, response, and recovery. Automation in these areas lowers mean-time-to-detect and reduces the potential for disruption or damage to key processes.

Resources can also be allocated in more efficient ways with AI augmenting human capabilities and allowing smaller teams to manage complex CPS environments.

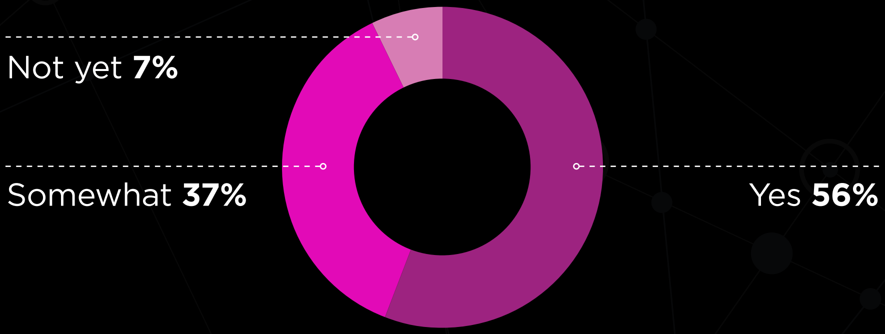
Tactically, AI can bring efficiency gains in a number of ways:

- AI’s speed in analyzing sensor data and traffic can rapidly identify anomalies and threats to CPS environments, especially zero-day vulnerabilities yet to have been disclosed to and remediated by vendors.
- AI is also a powerful predictive threat detection tool that allows CISOs to strategize proactive defensive measures in the face of new threats.
- This may also include the identification of risky exposures such as misconfigurations that can be leveraged in attacks, or remediation of flaws that are most likely to be exploited first.

AI can also be an effective tool in incident response, by isolating compromised network segments or systems, blocking risky IP address ranges, and analyzing logs and alerts for other risky network behaviors.

93% of respondents consider AI at least somewhat of a requirement for CPS protection.

Do you consider AI capabilities a requirement for your cyber-physical systems (OT, IoT, IIoT, IoMT or BMS) security tools?



2. Compliance, Regulatory Changes—and a Coming Overhaul?

Uncertainty doesn't arise just from economic confrontations, but also from the potential for shifts in the regulatory landscape. The complexity has only grown since the start of the year.

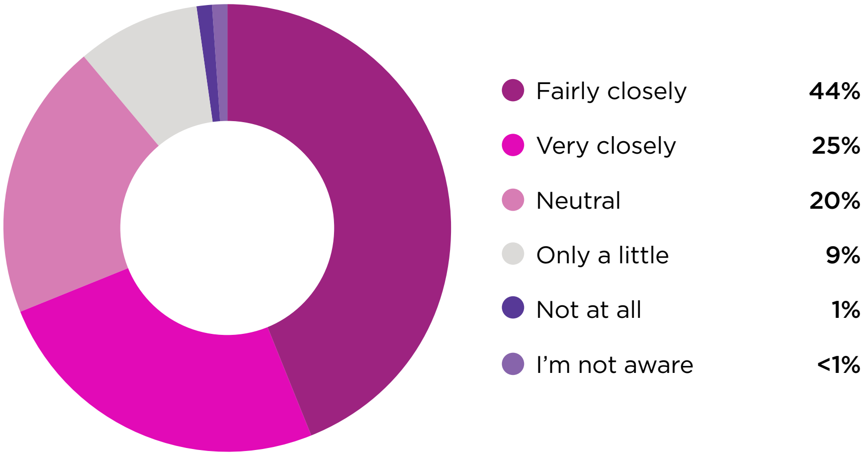
The Trump administration, for example, has indicated an appetite for deregulation through the rolling back of some Biden-era executive orders, including several mandates within EO 14144, whose aim was to strengthen and promote innovation in the country's cybersecurity.

While in Europe, the Cyber Resilience Act and NIS2 are mandates that enterprises in the European Union and United Kingdom are developing compliance initiatives in order to meet upcoming deadlines. NIS2 implementation deadlines, for example, vary by state, while CRA compliance features phased compliance deadlines aimed at a December 2027 full compliance deadline.

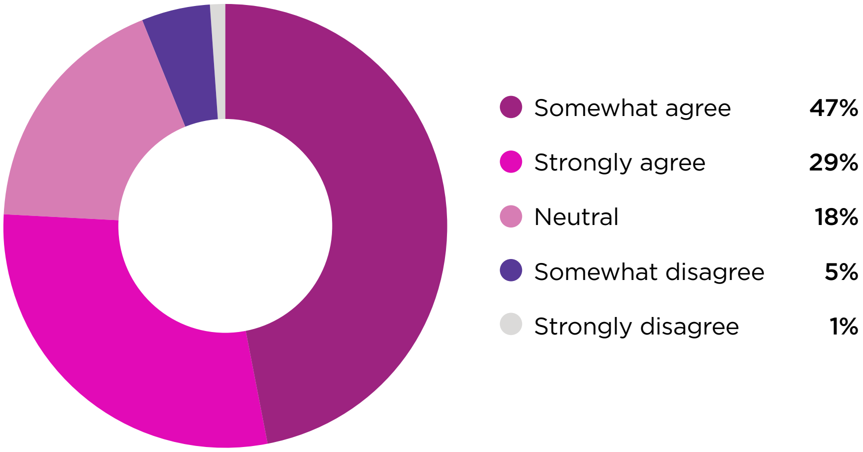
The offshoot is that CPS security programs built on established frameworks such as the NIST Cybersecurity Framework, or ENISA in the European Union, may soon be headed back to the drawing board. Disruption is expected to impact current compliance programs that are currently guided by a mix of industry standards and government regulations, according to respondents.

The large majority of respondents, meanwhile, believe that while their current CPS security strategies may adhere to regulations (69%), any upheaval in the regulatory landscape could upend existing investments and established best practices that ensure compliance (76%).

As of today, in your estimation, how closely is your cyber-physical systems (OT, IoT, IIoT, IoMT or BMS) security strategy adhering to evolving international and local cybersecurity standards or mandates?



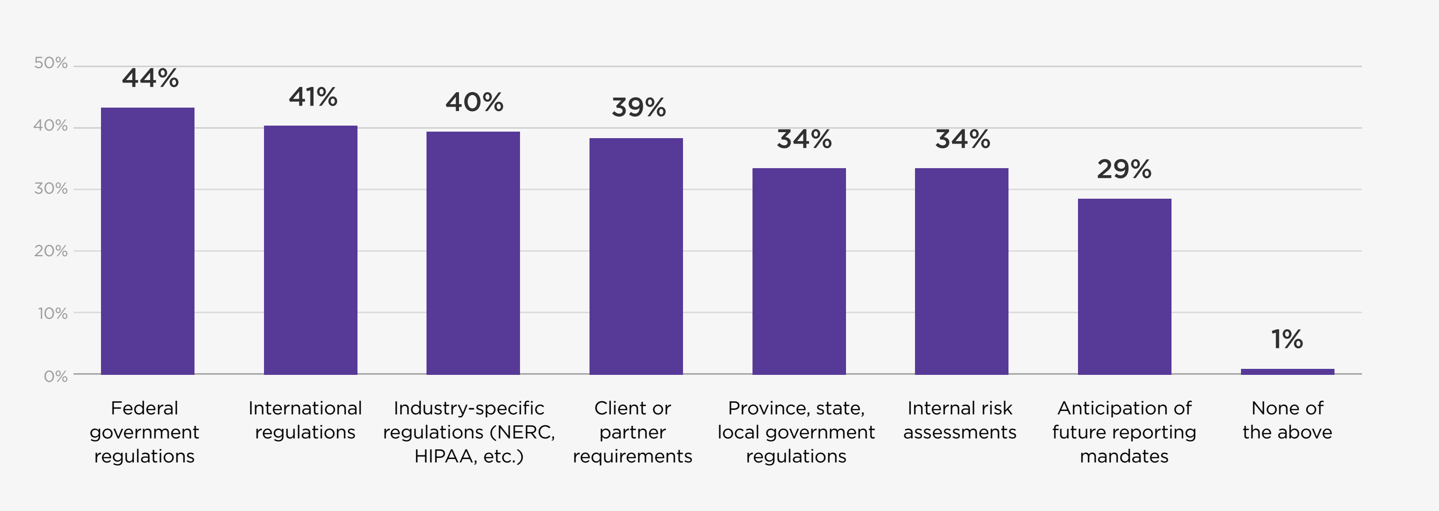
To what extent do you agree with the following statement: “Emerging compliance requirements, regulations or laws will require us to overhaul our current security strategy.”?



International, national, and industry-specific regulations mandate foundational CPS security controls and recommend adherence to established frameworks that guide programs. They provide a measure of accountability, oversight, and transparency from cybersecurity teams up through the board.

Tactically, regulatory requirements ensure that organizations formalize CPS risk mitigation with processes for exposure management, vulnerability remediation and mitigation, access controls, and incident response planning, among others. Some compliance requirements also extend these controls and transparency demands to supply chain partners and third-party vendors. Needless to say, regulations—in particular federal and international regulations—are the principal drivers of CPS security programs, rather than internal risk assessments, for example.

What are the primary drivers behind your organization’s current cybersecurity compliance initiatives?*



*Respondents were asked to select all that apply.

3. Security Teams, Business Leaders Taking a Second Look at Supply Chain Security, Remote Access

As noted earlier in this report, 67% of respondents are reconsidering their supply chain geography in order to mitigate risks to CPS posed by economic and geopolitical uncertainties. Should organizations be forced to make changes to their vendors and partners, suppliers' risk postures and technologies must be re-evaluated, and the window of exposure posed by these changes will be extended.

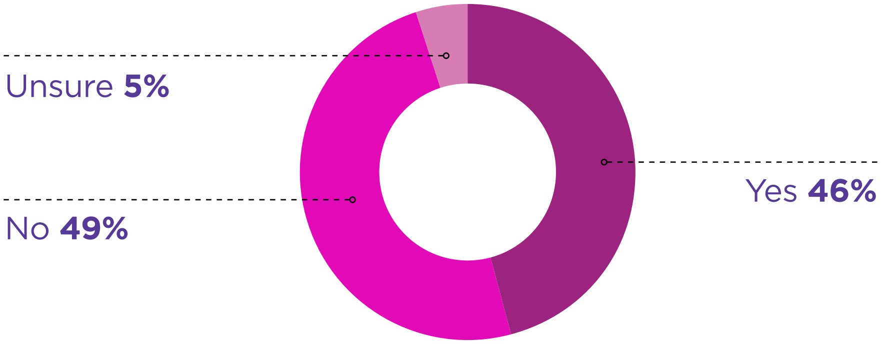
Attackers understand these ramifications all too well and could seize upon the risk introduced via this onslaught of new suppliers and technology in much the same way they did during the pandemic, by targeting the excessive remote access being afforded in order to keep businesses afloat.

Already in May 2025, we saw state-level attacks targeting supply chains. Reports surfaced then of a two-year campaign targeting logistics, defense, and technology companies that were part of the supply chain supporting Ukraine in its war against Russia. Russian military intelligence carried out attacks that compromised more than 10,000 surveillance cameras near critical transportation points in Ukraine and in the region surrounding it, the Associated Press reported. The aim was to learn more about the assistance coming into Ukraine from the West.

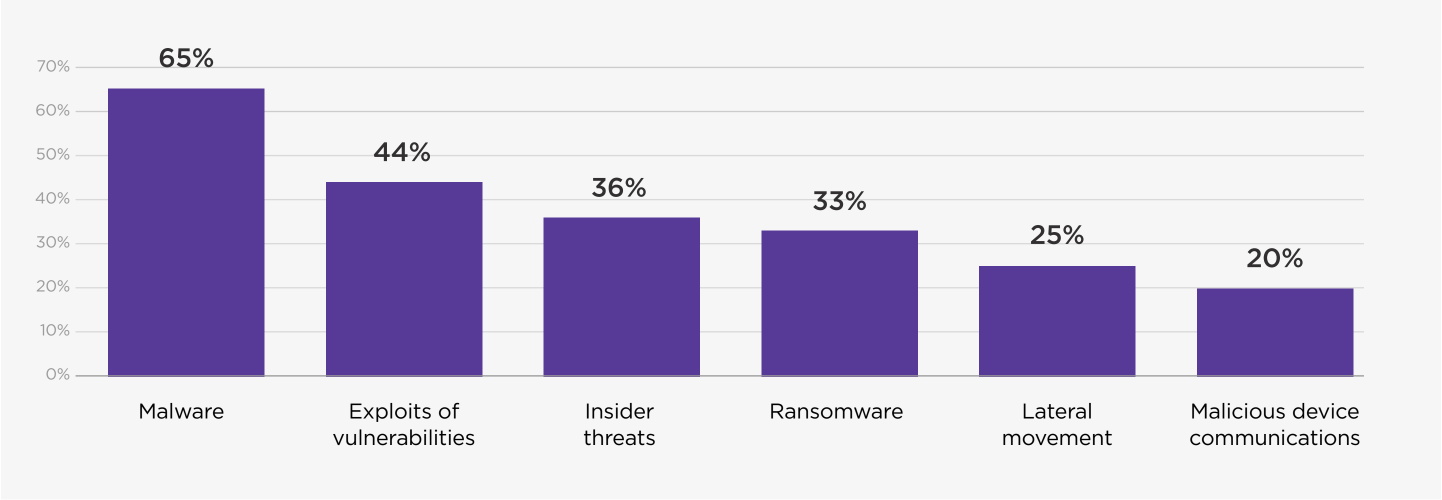
Supply chains and the digital infrastructure that support them can be fragile, and are targets for economic disruption and the destabilization of services within critical industries such manufacturing, logistics, pharmaceuticals, or food suppliers among many others.

46% of our respondents, for example, echo these concerns, reporting they had experienced breaches that leveraged third-party vendor access as an initial entry point to the network. These attacks led to malware, including ransomware being installed, disrupting business operations along the way. Attackers were also able to exploit vulnerabilities by using the access afforded a compromised supplier or partner.

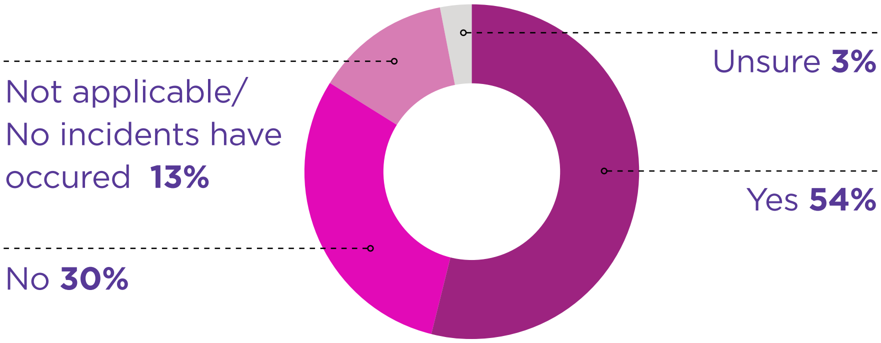
Has your organization experienced a cybersecurity breach in the past 12 months caused by third-party vendor access?



Which attack methods or types were used in the breach(es)?*



Has your organization ever discovered security gaps or weaknesses in vendor contracts after a cybersecurity incident occurred?



As cybersecurity teams focus on resilience, and ensuring that critical systems withstand incidents without a negative impact on the business, locking down remote access is an important first step. Attackers have become proficient at using phishing campaigns, brute-force attacks, and other tactics, techniques, and procedures (TTPs) in order to exploit exposed and poorly secured remote connections. From our results, respondents reported that risk reduction, cost savings, and visibility into remote activity on the network are the top factors driving this re-evaluation of remote access to CPS operations.

Which factors contributed to the decision to re-evaluate remote access to operations that contain cyber-physical systems (OT, IoT, IIoT, IoMT or BMS)?*

Ability to reduce risk by re-evaluating remote access	46%
Cost savings by re-evaluating remote access	38%
Lack of visibility into third-party activity	33%
Breach from a third-party network	32%
Infrastructure project requiring us to re-evaluate remote access	29%
Compliance or regulatory mandates	26%
Concerns about threat actors using remote access to breach our environment	26%
Audit findings	25%
Concerns about insider threats	24%
Cost and complexity associated with our current approach	20%
Concern regarding proliferation of insider threats	19%
Rising internal demand for remote access	19%
Proliferation of third parties' remote access tools	8%

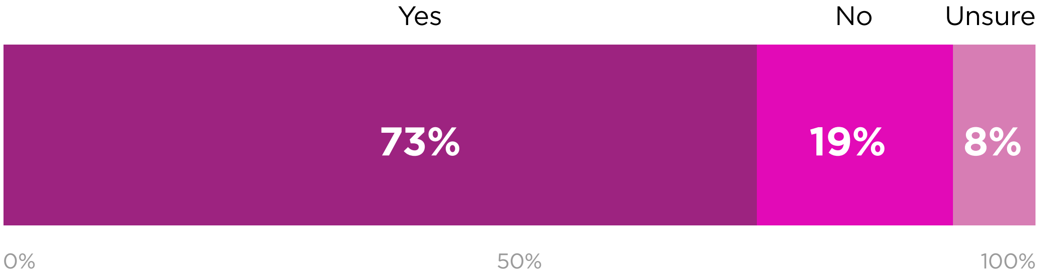
*Respondents were asked to select all that apply.

Securing remote connections to the enterprise network has been a decades-long challenge for security teams. Digital transformation has only ramped up the demand for external access to CPS, not only from employees, but also from third parties.

Organizations must consider the cybersecurity posture of third parties in particular when evaluating and prioritizing risk and assessing privileged access to systems. Many have in place, or are developing, risk-reduction activities to stem potential disruptions or failures resulting from unmanaged access.

Respondents said one area where enterprises can see an immediate risk reduction is through a re-assessment of remote access being granted to third parties, especially access to operations involving CPS, in order to contain risks. Nearly three-quarters of respondents are currently re-evaluating third-party remote access to CPS operations.

Is your organization re-evaluating third party remote access to operations that contain cyber-physical systems (OT, IoT, IIoT, IoMT or BMS) assets?



Many of the risk-reduction efforts respondents cited should be considered standard cybersecurity practices, but are often complex, drawn-out projects involving numerous lines of business that define roles and responsibilities, and the access required for internal employees and outside suppliers and partners to adequately do their jobs.

Nearly half of our respondents (49%) identified regular security audits as the top risk-mitigation activity on their agendas. Remote access security audits evaluate the effectiveness of existing controls in order to prevent unauthorized access to, and the availability and integrity of, CPS assets, Audits can be expansive and include security testing of remote devices such as off-the-shelf and enterprise-grade remote access solutions, penetration testing in order to identify exploitable vulnerabilities, and assessments on policy enforcement.

In addition to regular audits, process improvements for providing change approvals were cited by 45% of respondents. These may include streamlined approvals for remote access requests, and policies that define controls such as multifactor authentication, enforcement of the principle of least privilege, encrypted connections, and regulatory compliance.

How is your organization mitigating risk caused by increased access to cyber-physical systems (OT, IoT, IIoT, IoMT or BMS) networks?

Regular security audits	49%
Process improvements for providing change approvals	45%
Identity management and governance programs	40%
Limit access to domestic suppliers and vendors	36%
Implemented multifactor authentication for third parties	33%
Improved due diligence for granting access to third parties	33%
Introduced secure access controls	27%
Conduct continuous monitoring of vendor access	11%

*Respondents were asked to select all that apply.

Current Controls

We asked which device types organizations were confident in securing using current third party remote access solutions.*

62%	52%	37%	35%	21%
Operational technology (OT)	Internet of things (IoT)	Internet of medical things (IoMT)	Industrial IoT	Building management systems (BMS)

*Respondents were asked to select all that apply.

Recommendations

Economic instability inevitably brings friction when it comes to managing CPS risk. In the face of intensifying threats from adversaries and a shifting regulatory environment, it may be time for enhanced strategic collaboration between cybersecurity leaders responsible for CPS protection and business leaders. We recommend a collective focus on prioritizing mitigation and remediations for the systems that have the most impact on business if disrupted because of a cyberattack.

This would be somewhat a reversal of current approaches, which are largely asset-centric. An asset-centric approach takes the device information gleaned from visibility tools and provides an understanding of all assets and their overall risk. This is a necessary first step and is imperative when considering risk reduction, but an asset-centric only approach can lead security analysts to prioritize risks that would have little to no impact on the business if exploited. An asset-centric approach to risk reduction doesn't take business impact into account, only the device properties.

Structure Risk Reduction Based on the Impact to Business Outcomes

With tariffs and trade restrictions impacting global markets, and kinetic fighting threatening further disruptions, it's an opportune time for organizations to fundamentally shift how they approach CPS risk reduction.

By taking an impact-centric approach to risk reduction, system owners and business leaders would structure their CPS inventory the way they view the environment. Security teams are then enabled to prioritize risk reduction based on potential impact to business and regulatory outcomes. It also gives a shared language and mutual understanding of assets to the IT team and their OT and engineering counterparts.

This approach to CPS protection should not only reduce risk, but also enhance compliance efforts organization-wide.

Security teams have long struggled to speak the language of business leaders. They've clamored for seats among the C-suite and to have a voice with the board. But the dividing line of technology and business is a steep hill and few have managed to climb it effectively.

Adopting a strategy that starts with understanding risks to your environment in the context of how the business sees them—as production lines, building floors, hospital wings—brings an unmatched perspective to CPS protection and cybersecurity, and can help traverse that boundary between security, compliance teams and business leaders. By focusing on the potential business impact of risks, security teams can confidently know they are achieving the business goals of preventing disruption, downtime, and financial loss.

Three Outcomes of an Impact-Centric Approach to CPS Security

Impact-Centric Risk Reduction

The prioritization of security issues should hinge in part on the asset's business context. A critical vulnerability in a programmable logic controller (PLC) or medical system should be addressed, but the recommendation need not be to schedule downtime for an entire production line of PLCs or a fleet of hospital imaging systems. Sufficient context allows security teams to prioritize remediation to address issues within devices that have the greatest business impact first.

This takes on greater significance in sectors such as healthcare where life-support machines are one example of a device generating critical resources while in parallel being responsible for the greatest revenue stream. These areas should be prioritized and protected, reducing risk while demonstrating a viable business for investments in CPS protection.

Contextual Prioritization

CISOs and their teams are gaining responsibility for securing CPS environments in many organizations. These teams need a way to know what an asset does so they can understand why an alert matters beyond details of a vulnerability, risky configuration, or a policy deviation.

This calls for the construction of device purpose hierarchies, which is the categorization of CPS assets in a taxonomy that makes sense in the enterprise's industry. Any risk scoring would have to be derived from a custom business impact analysis. Security analysts can then immediately apply that hierarchy in order to understand the potential business impact of an alert in the CPS environment, which allows them to appropriately prioritize fixes.

Risk Benchmarking and Business Comparisons

In an unstable economy, budgets are scrutinized in great depth. The ability to accurately identify, assess, and prioritize risk across connected devices is the foundational aspect of providing an overall view of your organization's security posture. It's important that security teams have a broader perspective on exposures and that security teams have a greater understanding of the state of their organization's unique risk posture. By performing industry benchmarking, business leaders and decision makers can have a proper understanding of how an enterprise stacks up against its peers. These types of exercises allow teams to visualize how critical assets are covered, and informs measurements of risk reduction efforts over time—another essential for boards and business leaders.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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.