CLAROTY

SURVEY REPORT

The Global State of CPS Security 2024: Business Impact of Disruptions

An analysis of the financial and operational impact of cyberattacks affecting mission-critical infrastructure

Executive Summary

Claroty presents the results of an independent global survey of 1,100 cybersecurity professionals who are tasked with securing cyber-physical systems (CPS)—including operational technology (OT), Internet of Things (IoT), connected medical devices (IoMT), and building management systems (BMS)—that are at the core of critical infrastructure sectors worldwide. The survey sought to understand from cybersecurity leaders their experiences combating cyberattacks affecting CPS, particularly focusing on the financial impact and business disruptions resulting from incidents. Key findings include:

1. Cybersecurity Incidents Affecting CPS Result in Steep Financial Losses

- Nearly half of respondents (**45%**) reported a financial impact of $500,000 USD or more in the last 12 months from cyber attacks affecting CPS, with over a quarter (**27%**) reporting $1 million or more.
- Several factors contributed to these losses, the most common being lost revenue (selected by **39%** of respondents), recovery costs (**35%**), and employee overtime (**33%**).
- The most financially impacted sectors are chemical manufacturing, power and energy, and mining and materials, with **54-55%** of respondents in each sector reporting more than $500,000 in losses from incidents in the last 12 months.

2. Ransomware Still Plays Heavily into Recovery Costs

- Over half of respondents (**53%**) met ransom demands of more than $500,000 USD to recover access to encrypted systems and files in order to resume operations.
- This problem is particularly severe in the healthcare sector – **78%** reported ransom payments over $500,000 – as ransomware and extortion-based attacks on hospitals and clinical environments continue to run seemingly unabated.

Top Financial Impact Contributors:

- Lost Revenue
- Recovery Costs
- Employee Overtime

$

78%

of healthcare organizations paid $500,000+ in ransom payments in the last year

3. Consequential Operational Impacts Felt by Organizations Worldwide

- Nearly half of respondents globally (**49%**) experienced more than 12 hours of operational downtime resulting from a cyberattack in the last year, and one-third (**33%**) reported at least a full day of downtime.
- About half (**49%**) said the recovery process took a week or more and nearly a third (**29%**) said recovery took over a month.
- The most common cybersecurity impacts are process manipulation (selected by **38%** of respondents) and process disruption (**37%**), which go hand-in-hand with operational downtime.

4. A Remote Access and Supply Chain Problem

45% of respondents said at least half of their organization's CPS assets are connected to the internet, as increased connectivity and convergence have exacerbated the need for remote access to CPS. The most common connection method is through a virtual private network (VPN)—selected by **36%** of respondents—which lack CPS-specific security controls.

82% of respondents said at least one cyber attack – and nearly half (**45%**) said five or more attacks – in the past 12 months originated from third-party supplier access to the CPS environment. And yet, almost two-thirds (**63%**) admit to having only partial or no understanding of third-party connectivity to the CPS environment.

5. Resilience Strategies are Paying Off in Risk Reduction

Respondents expressed growing confidence in their organization's risk reduction efforts, indicating a growing maturity around the defense of CPS environments and a deeper understanding of their impact on critical infrastructure.

Most respondents (**56%**) have greater confidence in the ability of their organization's CPS to withstand cyber attacks today versus 12 months ago. Additionally, **72%** expect to see quantifiable improvements in their CPS security in the next 12 months.

49%

experienced 12+ hours of operational downtime due to cyber attacks in the last year, while recovery process took a week or more

82%

experienced at least one cyber attack that originated from third-party access to the CPS environment

Introduction

Cybersecurity leaders understand full well the ramifications of cybercrime and advanced attacks against the cyber-physical systems (CPS) that underpin industrial and healthcare computing infrastructures. Cyberattacks, whether state-sponsored or carried out by for-profit criminals, have increasingly targeted operational technology (OT), Internet of Things (IoT), connected medical devices (IoMT), and building management systems (BMS). These incidents have caused process disruptions, service delivery delays, data loss and data manipulation, and other negative outcomes that can affect anything from patient care and public safety, to national and economic security.

Meanwhile, CISOs in critical infrastructure sectors such as manufacturing, healthcare, energy, oil and gas, and others often find themselves trapped in a hamster wheel of pressures applied by threat actors and business leaders as they try to manage risk and mitigate threats. As they commiserate with the C-suite and boards of directors, security leaders must articulate threats in the context of risks to the business – i.e., how much they cost.

To counter that dynamic and hopefully ease those pressures, this survey report seeks to quantify the cybersecurity and operational impact of disruptive attacks to these critical systems, and provide context that cybersecurity leaders can leverage to strategize adequate protection for CPS.

To better understand the potential impact of disruption to cyber-physical systems in critical infrastructure sectors, Claroty's survey focused on the following areas:

- Financial setbacks to organizations as a result of attacks targeting CPS specifically
- Cybersecurity and operational impacts such as process manipulation or disruption, or system unavailability forcing expensive recovery costs
- Expansive risks introduced by excessive connectivity and unmanaged third-party access to critical systems
- Risk-reduction efforts implemented by enterprises in the past 12 months and their confidence in the effectiveness of those efforts

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 40 countries across the Americas, Europe, and Asia-Pacific, and more than a dozen industries, including automotive, chemical, food & beverage, healthcare, pharmaceutical and biotechnology, power and energy, transportation, and others.

Key Findings

1. CISOs Dealing with Excessive Financial Impact from Attacks Affecting CPS

Attacks against cyber-physical systems are no longer unicorns. Advanced attackers such as Russia's Sandworm APT and Iran's Revolutionary Guard Corps have launched very public cyberattacks against the electricity infrastructure in Ukraine and water treatment facilities in the U.S. and Israel, respectively. Ransomware, meanwhile, remains a clear and present threat to hospitals and the sanctity of patient care. Hundreds of attacks have impacted healthcare delivery organizations (HDOs)—most notably the Change Healthcare incident detected in February—and millions of dollars in ransom and extortion demands have been sent to attackers in the hopes of regaining access to, and control of, impacted patient data and medical devices.

There are severe financial implications for businesses that surround such incidents, many of which begin with commodity attacks against IT infrastructure and the enterprise network, ultimately impacting industrial processes or patient care, for example. Nearly half of respondents (**45%**) reported a financial impact of $500,000 USD or more in the last 12 months from cyber attacks affecting CPS, with more than a quarter (**27%**) reporting $1 million or more.

Our respondents noted numerous, specific financial implications starting with lost revenue, recovery costs associated with either ransom payments, or other technical charges such as reimaging of servers and endpoints, and less quantifiable costs such as the impact on brand and business reputation.

Globally, **39%** of respondents cited lost revenue as the top financial impact; **27%** reported a financial impact of $1 million (USD) or more in the last 12 months, with 12% claiming to have lost $5 million or more as a result of incidents.

Estimate the financial impact of the cyberattacks your organization has experienced in the past 12 months in USD lost:

Less than $100,000	**19%**
$100,000-$499,999	**22%**
$500,000-$999,999	**18%**
$1,000,000-$4,999,999	**15%**
$5,000,000 or more	**12%**
No financial impact	**14%**

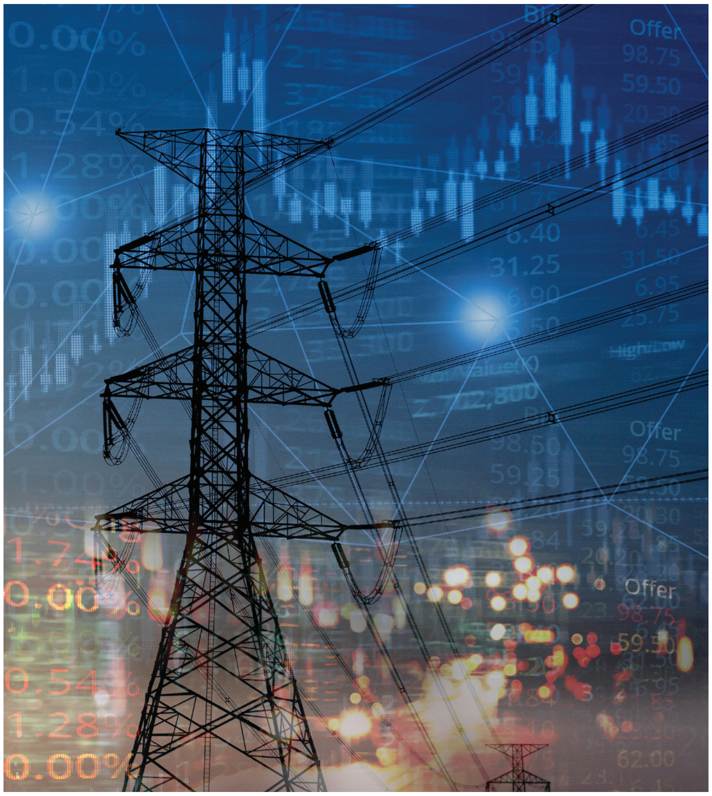
A percentage sample of reported losses of $1 million or more by industry:

Power and energy	**38%**
Mining	**32%**
Transportation	**30%**
Food & Beverage	**29%**
Chemical	**26%**
Healthcare/Pharma	**26%**

The contributing factors, meanwhile, are varied:

Which factors contributed to the financial impact? (multiple selections permitted)

Revenue lost	**39%**
Recovery costs	**35%**
Employee overtime	**33%**
Legal fees	**31%**
Loss of customer or partner relationship(s)	**30%**
Incident response / forensics	**29%**
Ransomware payments	**28%**
Regulatory fines	**28%**
Brand reputation recovery costs	**27%**
No financial impact	**4%**

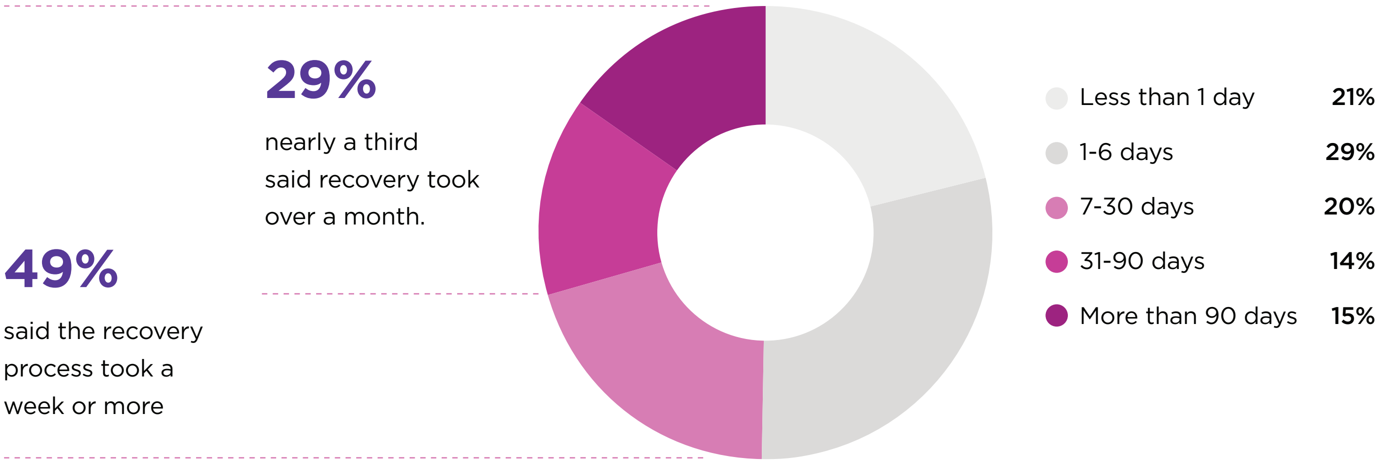


2. Of Recovery Costs and Ransomware

Beyond lost revenue, respondents cited recovery costs as the second most significant factor contributing to the financial impact of cyberattacks on CPS. Incidents impacting manufacturing, power and energy, or healthcare organizations, for example, can result in long recovery times. Organizations are often faced with recovering from known, good backups in the case of disruptive ransomware attacks or destructive attacks from a state actor. Servers must be re-imaged, mitigations applied, and remediation steps such as patching and firmware updates must be taken.

In some cases, this results in lengthy downtime or systems unavailability, which often can impact public safety or patient care in the case of healthcare delivery organizations. About half of respondents (**49%**) said the recovery process took a week or more and nearly a third (**29%**) said recovery took over a month.

How long was the recovery process?



Ransomware continues to be the worst scourge plaguing companies in critical infrastructure sectors. Losses and downtime pile up quickly, and recovery efforts such as backups are rapidly put to the test under the most stressful of circumstances. Costs here are also quantifiable with organizations—despite recommendations from law enforcement and cybersecurity experts alike—often making the difficult business decision to negotiate with and meet an attacker's ransom demands.

These attacks, meanwhile, have evolved. No longer are these exclusively attacks that encrypt critical systems and information; they are often secondary attacks paired with data breaches and theft of intellectual property. The stolen data is held over a victim's head with the attacker threatening to leak patient data or lost business information in an attempt to extort even more from the compromised company.

Meanwhile, ransom demands and related recovery efforts continue to be among the costliest impacts from cyberattacks, especially against mission-critical infrastructure such as CPS.

For example: globally, more than half of organizations (**53%**) met ransom demands of more than $500,000 USD, while **16%** shelled out $5 million or more to recover access to encrypted systems and files in order to resume operations.

Within the healthcare sector, where ransomware and extortion-based attacks continue to run seemingly unabated, **78%** reported ransomware payments of $500,000 USD or more.

How much did your organization pay in ransomware payments?

	All Sectors	Healthcare
Less than $100,000	**14%**	**—**
$100,000-$499,999	**21%**	**11%**
$500,000-$999,999	**20%**	**39%**
$1,000,000-$4,999,999	**17%**	**39%**
$5,000,000 or more	**16%**	**—**
My organizations did not pay any ransoms	**13%**	**11%**

59% of organizations in Europe reported at least $500,000 in ransomware payments, with 23% meeting ransom demands between $1 million and $5 million.

Cyber insurance, meanwhile, continues to gain momentum as companies attempt to offset some of the costs associated with attacks. Brokers and insurance providers, however, are becoming stringent about requiring certain controls be in place before providing coverage. Gaps in cybersecurity programs such as a lack of standardized practices, a lack of incident response plans, and other shortcomings could render some companies—especially small businesses and midmarket enterprises—uninsurable.

Yet, globally, respondents reported some hefty payouts from cyber insurance coverage post-incident, helping to offset some of the steepest recovery costs.

How much did your cyber insurance policy award you in the past 12 months?

Less than $100,000	17%
$100,000-$499,999	20%
$500,000-$999,999	19%
$1,000,000-$4,999,999	19%
$5,000,000 or more	14%
My organization does not have cyber insurance	11%

3. Consequential Operational Impacts

It's clear that cyber-physical systems (CPS) are essential to public safety, national security, and economic stability—and equally clear they have become prime targets for extortionists, hacktivists, and saboteurs intent on exploiting weaknesses in legacy technologies and excessive connectivity for profit or geo-political gain.

Late last year, intrusions at water treatment facilities in the United States and Israel exploited weaknesses in Israeli-made industrial control systems, allowing a group believed to be associated with Iran's Revolutionary Guard Corps access to these systems. While these integrated Unitronics programmable logic controllers and human machine interfaces (PLC/HMI) controllers were only defaced, the attacks were meant to sow chaos and fear in the integrity of water quality control systems.

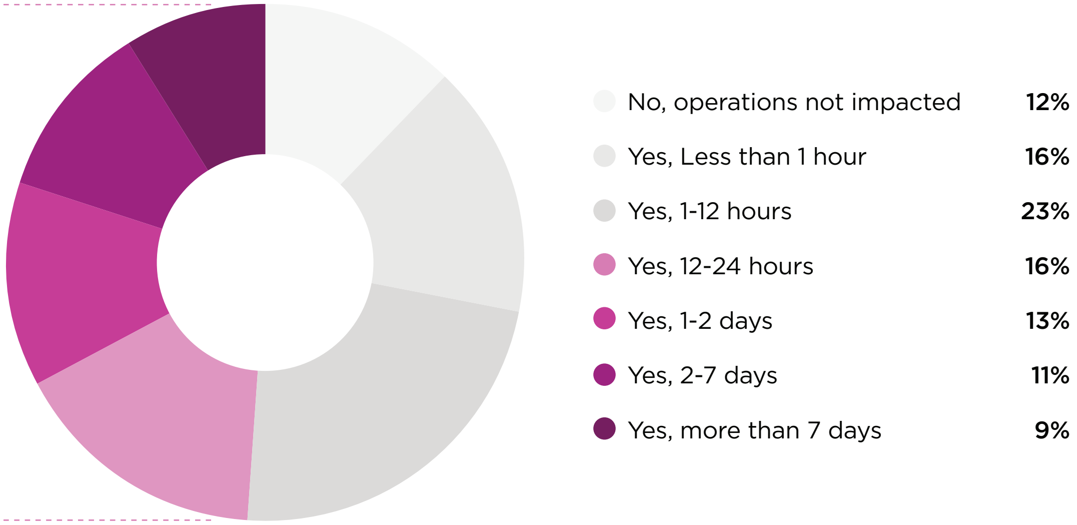
Ransomware attacks against hospitals have been highly publicized, especially in instances where patients are diverted to other facilities, or scheduled surgeries are forced to be postponed or canceled because critical patient data or connected medical devices are unavailable.

Globally, respondents were candid about the operational and cybersecurity impacts from attacks against CPS. CPS environments are hallmarked by their intolerance for downtime, yet nearly half (**49%**) of respondents globally experienced more than 12 hours of operational downtime resulting from a cyberattack, and one-third reported at least a full day of downtime.

In the past 12 months, has your organization experienced cyberattacks that resulted in operational downtime that impacted your organization’s ability to produce goods or services? If yes, how long did the downtime last?

49%

of respondents globally experienced more than 12 hours of operational downtime



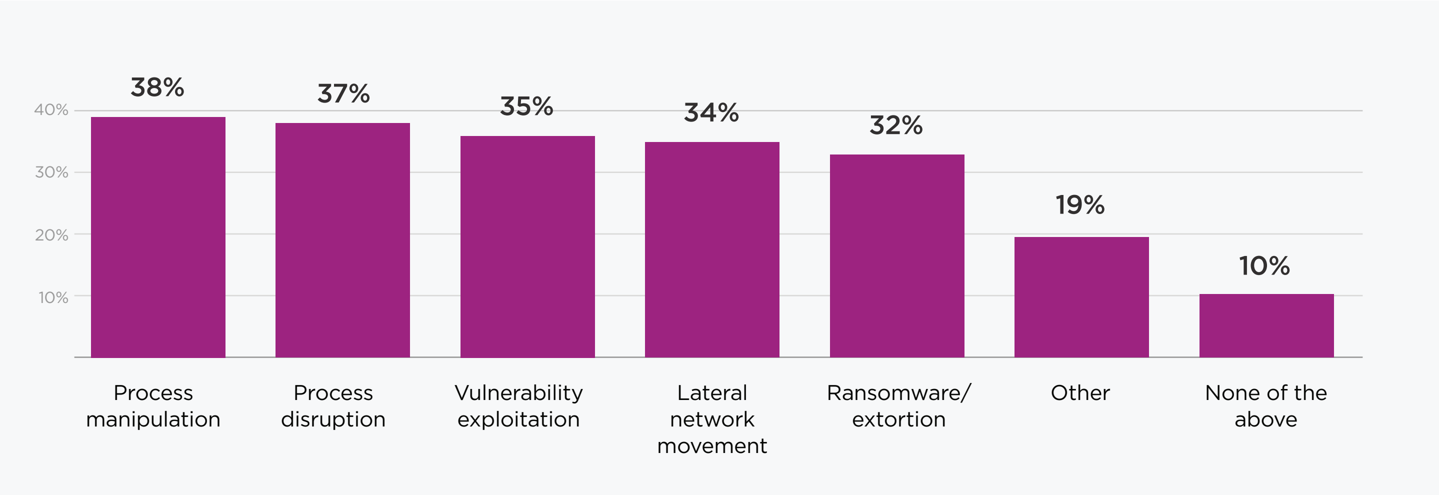
Industrial, manufacturing, and other processes that are disrupted or manipulated can severely affect system availability or the safety of operators or the public. This can force production shutdowns or delays in product delivery, adding up to costly financial losses.

What was the operational impact of cyberattacks against CPS (multiple selections permitted)?

Financial losses	**38%**	Legal implications	**23%**
Reputational damage	**32%**	Staffing changes	**22%**
Product delivery shutdown	**30%**	Public safety	**21%**
Production shutdown	**28%**	Patient care disruption	**20%**
Loss of customer/partner relationship	**28%**	Human injury	**17%**
Loss of intellectual property	**27%**	Other	**15%**
Regulatory implications	**25%**	None of the above	**5%**

Disturbingly, process manipulation was the top impact resulting from a cyberattack cited globally by **38%** of respondents. Process disruption, hand-in-hand with downtime, was the next most-cited impact at **37%**, more so than successful exploits of known and unknown vulnerabilities, lateral network movement from CPS to the enterprise network, and even ransomware and extortion attacks.

What was the cybersecurity impact of the attack(s) (multiple selections allowed)?



Which of the following consequences from cyberattacks has had the longest-lasting effect on your organization?

Data loss or manipulation	**19%**
Data privacy violations	**15%**
Inaccessible systems and information	**13%**
Irrecoverable systems and information	**13%**
PHI/PII loss	**10%**
Extortion	**9%**
None of the above	**8%**
Compliance violations	**7%**
Other	**6%**

4. The Problem with Third-Party and Remote Access Exposures

Organizations are feeling pressure to meet demands for remote access to CPS (**45%** of respondents said at least half of their CPS assets are connected online). Whether it's from employees or third-party suppliers and partners, organizations are doing so, in some cases, in ways that create additional exposures and risk to the business.

Our survey numbers reveal some of their less-than-best practices. For example, globally, **32%** of respondents admitted to directly connecting CPS to the internet, via exposed open ports and other poorly held cybersecurity practices. Most connect through a virtual private network (VPN) solution (**36%** of respondents), however most VPNs are generally an insufficient means of remotely connecting to industrial control systems or medical devices.

VPNs, jump boxes, and non-enterprise grade remote access solutions lack the session recording, auditing, and role-based access controls that would be necessary to properly defend an OT environment. Some lack basic security features such as multi-factor authentication (MFA) options, or have been discontinued by their respective vendors and no longer receive feature or security updates.

Research published in May and September 2024 by Claroty Team82 demonstrates on two fronts some of the potential weaknesses caused by insecure connectivity that attackers could leverage. For example, on the OT side, critical Windows-based engineering workstations and human-machine interfaces (HMIs) were often directly connected to the internet, rather than through a secure remote access solution.

This introduces unnecessary risk since this type of connectivity allows attackers to easily discover the presence of these devices on the internet and enables brute-force attacks in order to access them. Many of these devices also contain known exploited vulnerabilities, exponentially increasing their exposure and risk.

How are CPS connected to the internet in your organization? (multiple selections permitted)

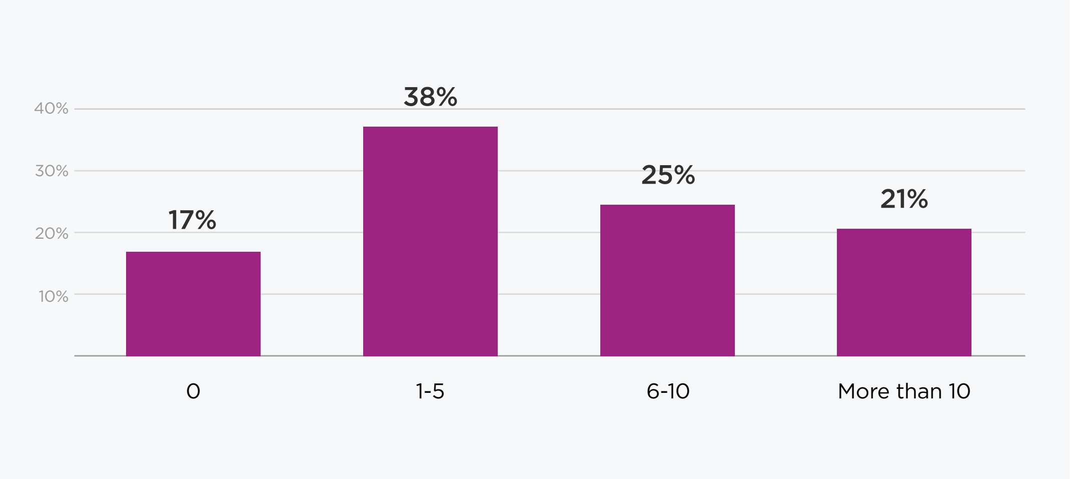
Through a virtual private network	**36%**
CPS-specific secure remote access tool that we own	**32%**
Remote desktop protocol	**32%**
Direct connection to the internet (open ports)	**32%**
TeamViewer or remote management tool	**32%**
CPS-specific secure remote access tool provided by a third-party	**28%**
Through a jump box	**27%**
None of the above	**8%**

Organizations also have a problem with sprawl, combating this need for remote access with an excessive amount of technology—much of it not necessarily built with security in mind. **55%** of organizations in Team82's dataset are running four or remote access tools (**33%** running six or more). Meanwhile, **79%** have two or more non-enterprise grade tools installed on devices running on the OT network. Among those non-enterprise grade tools are TeamViewer and AnyDesk, both of which have suffered breaches this year; **89%** of companies in our dataset have TeamViewer deployed, **63%** have AnyDesk in their environments.

Such sprawl expands the available attack surface available to threat actors, and adds a significant operational burden to manage and secure these tools.

These demands for remote access are born out of both the need to support converged environments and the plethora of vendors, partners, and suppliers that require access in order to manage these systems, conduct maintenance, and apply feature or security updates. Globally, our survey respondents fall in line with Team82's findings.

How many remote access tools are currently in use in your CPS environment?



45%

of CPS are connected to the internet directly or indirectly.

Many of these remote connections are requirements of third-party relationships, yet globally, **63%** of respondents said they have only partial or no understanding of third-party connections to their CPS environments. Another **21%** said they had limited control over who can connect into a CPS environment.

These are crucial numbers when it comes to the integrity of the supply chain and remote connectivity from third parties. Often, organizations have little visibility into a supplier's cybersecurity practices, or have limited contractual power in these relationships to make certain requirements. In the meantime, a compromised third party, as evidenced by the Change Healthcare attack, SolarWinds, NotPetya, and other incidents can prove to have devastating consequences to organizations industry-wide.

Change Healthcare, for example, reported that it had detected a breach and ransomware attack in February 2024. Change is the healthcare industry's largest claims payment processor, and its systems were offline for several weeks, leaving claims unprocessed and some medical providers in financial distress without compensation for services rendered. A compromise of this one hub in the overall healthcare ecosystem proved to have significant financial impacts.

A survey published in April by the American Medical Association painted a picture of the disruptions from the attack, noting that **80%** of medical practices lost revenue from unpaid claims or claims they were unable to submit. Respondents also reported delays in claim repayments or an inability to check for benefit eligibility.

Our survey revealed that **82%** of respondents said at least one cyber attack – and nearly half (**45%**) said five or more attacks – in the past 12 months originated from third-party supplier access to the CPS environment. Globally, **38%** of our respondents across industries reported between one and five cyberattacks originating from third party access to the environment, **27%** reporting between five and 10, and **17%** reporting more than 10.

Some respondents, however, were able to improve relationships with third parties post-breach.

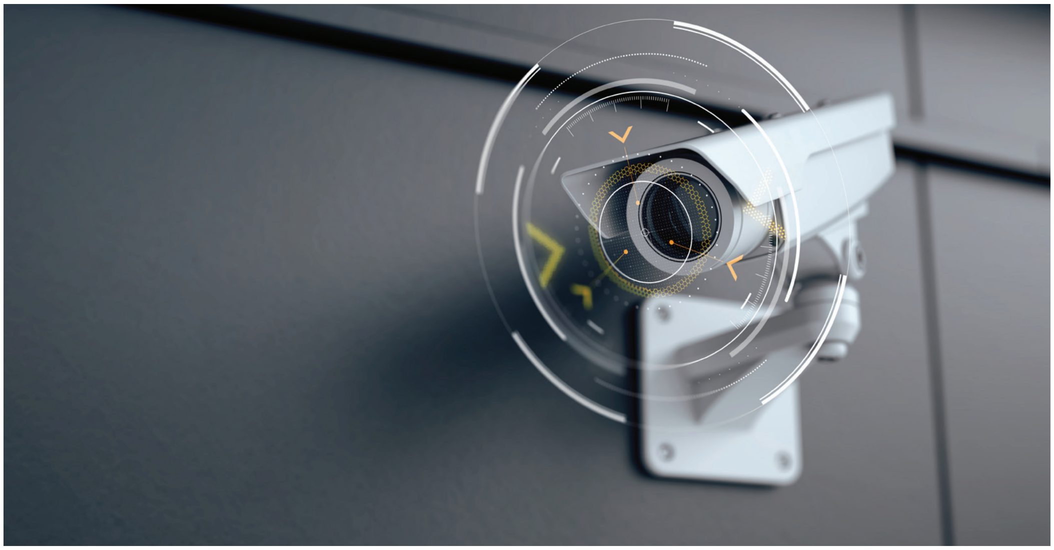
Did any of these cyberattacks negatively impact your relationship with the associated vendor/partner?

Yes – established new security protocols with them	**26%**
Yes – re-negotiated terms or pricing with them	**25%**
Yes – ended the relationship	**15%**
No – the relationship was unchanged	**15%**
N/A – none of the cyberattacks originated from third-party access	**19%**

While most cybersecurity incidents involving third parties have downstream implications, our survey also shows some upstream effects. **40%** of respondents said that between one and five attacks originating from their organizations impacted a third-party vendor environment. **19%** reported more than 10 attacks having such an impact.

26%

said new security protocols were established with a third party after an attack impacted the supply chain partner's environment.



5. Growing Confidence in Risk-Reduction Efforts

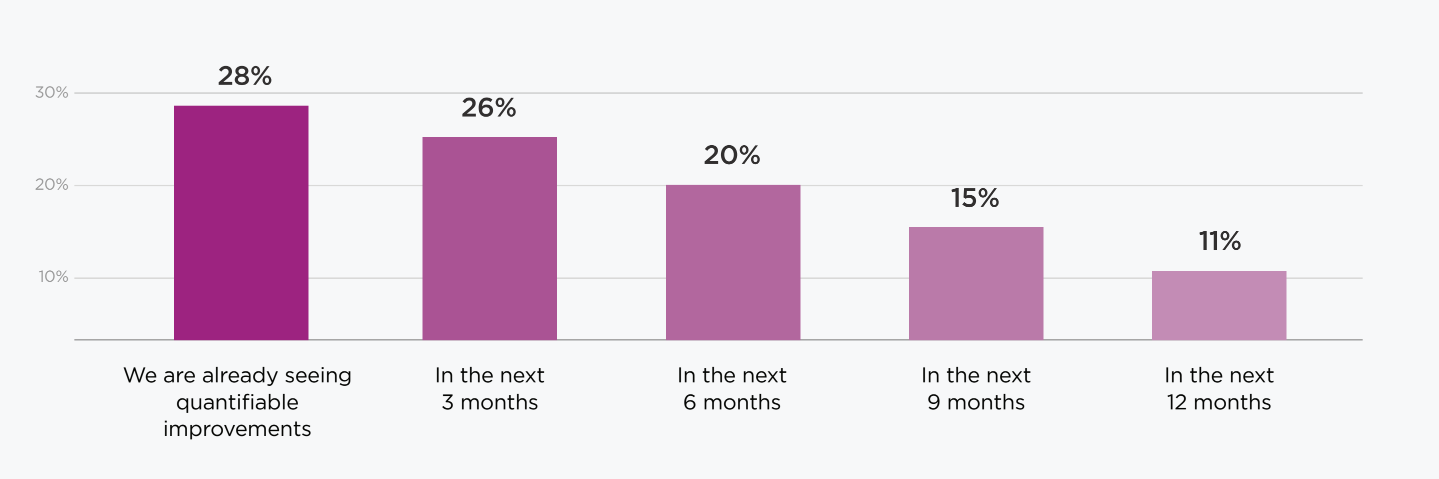
Defending cyber-physical systems from cyberattacks requires approaches that stray from IT security management. Organizations are strategizing to build resilient systems; they acknowledge that incidents are inevitable and architect systems and networks that can stand up to attacks, rather than try to boil the ocean by patching every vulnerability and addressing every known and unknown threat.

Most CPS environments recognize the need for accurate and ongoing asset inventory and visibility into connected assets, and to detect threats and unusual access to systems, prioritize remediation according to system criticality and known exploits, and comply with industry regulations by following accepted standards.

When asked about any security capabilities they believed were missing that would have decreased the impact of cyberattacks in the past 12 months, the top answer was having a risk assessment to help manage risk more effectively (selected by **34%** of respondents), followed closely by vulnerability management (**32%**) and asset, change, and/or lifecycle management (**31%**).

However, respondents seem confident in their risk-reduction implementations in the past 12 months, indicating a growing maturity around the defense of CPS environments, and an understanding of their impact on critical infrastructure.

Based on your risk reduction efforts over the past 12 months, when do you expect to see quantifiable improvement in the security of your CPS?



Respondents, meanwhile, said ransomware/extortion attacks were the threats they were prioritizing in order to minimize CPS disruption. Also high on their priorities list were state actors focused on disruption or sabotage, and hacktivists.

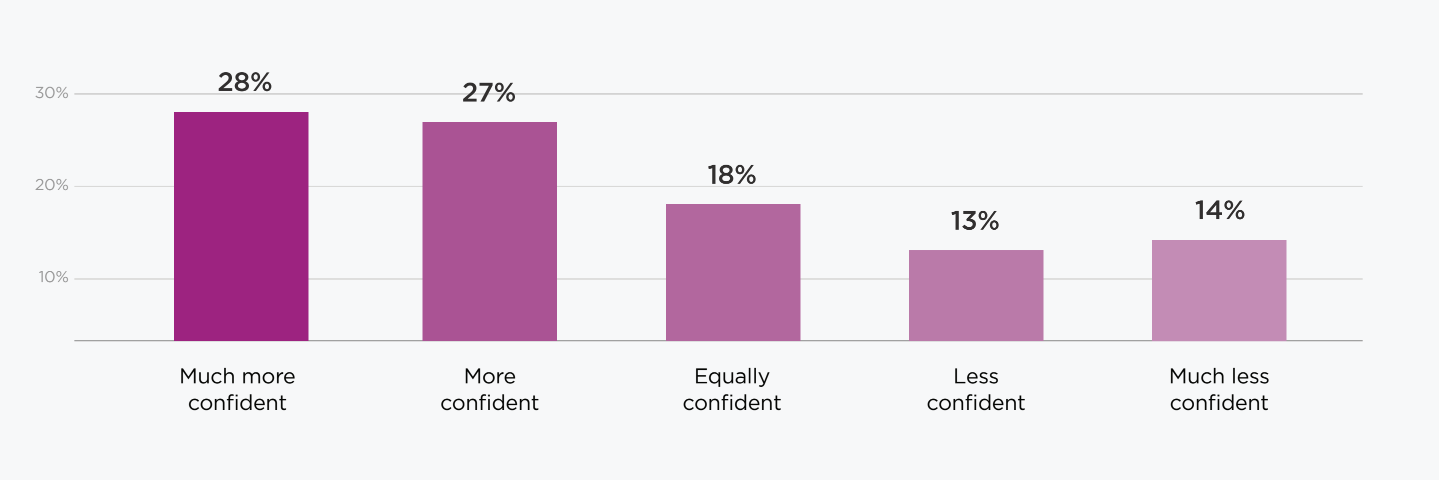
Which of the following threats do you prioritize to minimize CPS disruption (ranked in mean order of importance on a scale of 1-5, 1 being most important)?

1	Ransomware/extortion	**3.79**
2	State actors focused on disruption/sabotage	**3.81**
3	Hacktivists	**3.89**
4	Denial of service attacks	**4.03**
5	State actors focused on espionage	**4.09**
6	Insider threats	**4.16**
7	Human/operator error	**4.23**

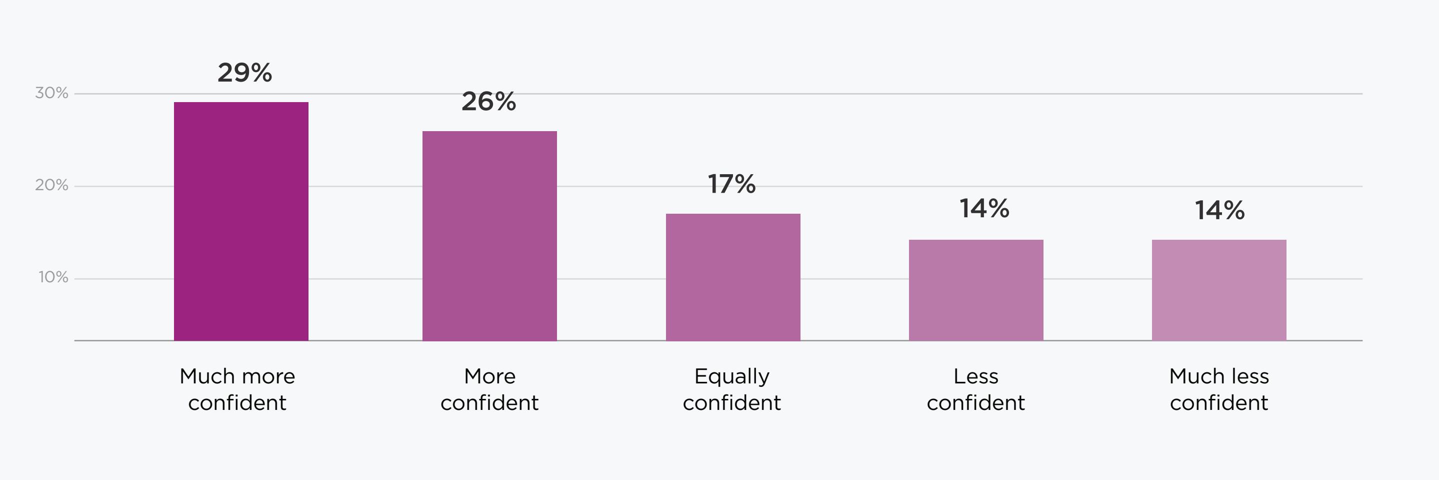
68% of respondents are “moderately” to “extremely” concerned about advanced state actors targeting CPS

As to the core capabilities of asset inventory and resilience, **56%** of respondents are reporting confident levels of their risk-reduction efforts in both areas.

How confident are you in your organization's visibility into all assets comprising your CPS today versus 12 months ago?



How confident are you in your organization's CPS' ability to withstand attacks today versus 12 months ago?



Recommendations

CISOs are increasingly challenged with new regulatory and personal legal pressures as part of their day-to-day responsibilities. Any business disruptions linked to a cyberattack can cast a harsh light on a cybersecurity program's effectiveness. Reducing risks to cyber-physical systems must be a priority for any cybersecurity leader given the ramped up connectivity of industrial control systems, smart devices and systems, and connected medical devices, especially due to the impact that a compromise to these systems can have in the physical world.

A focus on the following five areas can help guide security leaders as to what should be their desired end-state: resilient systems that withstand attacks and maintain the integrity and availability of production and services.

Asset Inventory

Exposure Management

Secure Access

Network Protection

Threat Detection

1. Asset Inventory

Successful cybersecurity programs hinge on asset inventory and visibility. Any value that is derived from any cyber-physical system (CPS) security program is dependent on the quality of its asset visibility. Organizations must identify all assets within the network, including hardware, software, applications, and data. This helps in understanding what needs to be protected.

Proper visibility allows for an understanding of the complex nature of CPS environments and the proprietary technologies underpinning OT, IoT, and connected medical devices. It also allows for better prioritization of exposure management, timely patching of the riskiest software and firmware flaws, and a reduction of overall risk.

2. Exposure Management

Exposure management is the lynchpin for modern cybersecurity programs. Organizations that are hyper-connected must understand where their weaknesses lie and prioritize them according to a number of factors, starting with exploitability, criticality of systems, lax access controls, and more. Risk assessments and business impact assessments are central to this strategy and leaders should understand the potential impact and likelihood of vulnerabilities being exploited, and prioritizing them based on their risk to the organization.

Security teams should recategorize high-risk devices based upon factors such as whether they are insecurely connected to the internet and contain vulnerabilities already exploited in the wild. This allows for the identification of devices and systems at highest risk of exploitation and significantly reduces the number and percentage of devices to be prioritized and mitigated.

3. Secure Access

Secure remote access for third-parties is a non-negotiable feature of today's CPS cybersecurity programs to ensure the security of user-to-machine communications. Organizations have exposed more technology and infrastructure to the internet than ever before. In return, analysts are getting better business metrics and deriving new efficiencies to cut costs and improve process efficiency, patient care, and other key services.

The offshoot of that, however, are more entry points to the network and increased exposure to both advanced and commodity attacks. Proper visibility feeds into a secure access strategy, and allows security leaders to understand whether control systems and other critical devices are securely connected to the internet, are protected by purpose-built remote access solutions, and guarded by strong access controls and privileged access management features. As we've seen in this survey report, organizations have reported the frequency of incidents as a consequence of poor third party access controls, and also an inordinate number of non-enterprise grade remote access tools deployed on the network.

These areas must be locked down and managed closely to ensure few business disruptions, costly revenue loss, and regulatory non-compliance is kept to a minimum. Many maturing organizations seek to establish a single CPS secure access hub that all vendors must use, creating a standard to maintain control and identity governance.

4. Network Protection

As CPS are increasingly leveraged to gain operational efficiencies, securing machine-to-machine and cloud workload-to-machine communications become critical functions to mitigate entire classes of cyber risk. As noted in our survey results, lateral movement is a core component of an attacker's methodology; they gain a foothold in an initial access point and attempt to access other systems and escalate privileges in order to steal data, deploy exploits, and malware such as ransomware.

Within CPS environments, organizations historically cited air gaps as a means of isolation. These mythical air gaps are usually non-existent as operators connect assets externally during emergencies or to accomplish work more efficiently. As organizations seek to gain the benefits of digital transformation, connectivity to IT or the public cloud is a requirement. Additionally IT/OT convergence requires enhanced connectivity. Whether in converged or non-converged environments, security leaders should look to leverage network segmentation as a means of ensuring secure communications. While an intensive endeavor, network segmentation is effective in limiting the ability of an attacker to move laterally. Secure network segments can also help isolate sensitive data and systems; such isolation can have compliance benefits as well in keeping company or customer information away from attackers.

CISOs and other leaders should begin the process by defining network segments based on security and compliance requirements and sensitivity, tune firewalls and access control lists accordingly to help with security policy enforcement. Finally, traffic monitoring and threat detection can also be prioritized accordingly to the sensitivity of particular network segments.

5. Threat Detection

Asset inventory and visibility into CPS assets provide an invaluable baseline not only to properly tune firewalls and access controls, but also to identify any deviations from accepted network traffic and activity on critical systems. Threat detection capabilities work in concert with the above recommendations in that once potentially harmful activities are detected, organizations can act on alerts and either isolate those affected systems or take actions to reduce risk in real time.

Advanced attackers and criminal entities are increasingly targeting CPS in order to cause disruption or, in worst-case scenarios, carry out destructive activity. It's crucial that industrial and healthcare organizations detect known threats and also understand anomalies in network and system behavior that could indicate a previously undetected threat, such as an exploit of a known exploited vulnerability.

Security operations centers (SOC) have integrations available for most threat detection technologies and can digest alerts in order to inform incident response activities. It's crucial to have this visibility into CPS in order to confidently—and centrally—manage threats to the environment in order to meet business requirements for uptime and preserve the integrity of data and systems core to the company's mission.

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.