INDUSTRY SNAPSHOT

The Global State of CPS Security 2024: Commercial

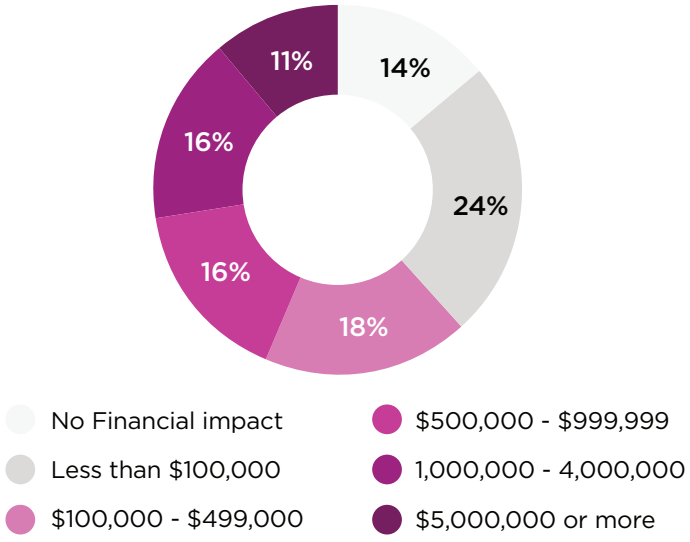
Cybersecurity leaders in commercial sectors including data centers, retail, hospitality, and commercial real estate dealt with significant challenges in 2024 when it comes to the protection of cyber-physical systems (CPS) including operational technology (OT), internet of things (IoT), and building management systems (BMS). Frequent and disruptive cyberattacks have resulted in significant financial costs and operational disruptions, delays in service delivery, data loss, and manipulations with far-reaching consequences for public safety and national and economic security.

To better understand how commercial organizations are responding to operational downtime, financial loss, and long recovery times due to cyber attacks, Claroty commissioned an independent global survey of 1,100 information security, OT engineering, clinical & biomedical engineering, and facilities management & plant operations professionals about the business impacts of cyber attacks on their organizations in the past 12 months.

Here are some insights from the 261 respondents who work in the commercial sector:

Cybersecurity Incidents Affecting CPS Result in Steep Financial Losses

When asked about the financial impact of cyberattacks to their organization, over 60% of respondents reported a financial loss of $100,000 or more. Nearly 30% reported a loss of $1 million or more. Several factors contributed to these losses, for the Commercial Real Estate industry revenue loss was the most significant factor (selected by 40% of respondents), for Data Centers recovery costs contributed the most (44%), and for Retail and Hospitality legal fees were the most impactful (41%).



Ransomware Still Plays Heavily into Recovery Costs

When asked how much their organization paid in ransom, alarmingly, over one-third (36%) of respondents met ransomware demands of $1 million or more to recover access to encrypted systems and files in order to resume operations. When considered alongside the hourly cost of downtime, it's easy to understand how a cyber incident could quickly rack up tens of millions of dollars in financial repercussions if not resolved immediately.

N/A - My organization did not pay any ransoms	**8%**
Less than $100,000	**16%**
$100,000 - $499,000	**29%**
$500,000 - $ 999,999	**19%**
$1,000,000 - $499,999,999	**9%**
$500,000,000 or more	**19%**

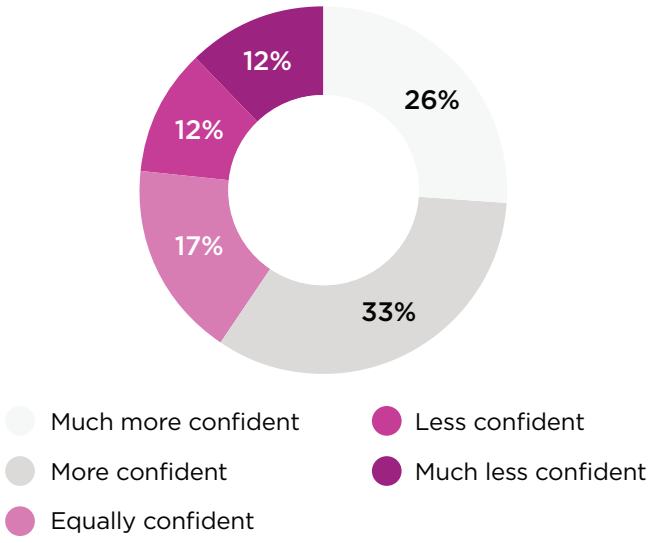
Consequential Operational Impacts Felt by Organizations Worldwide

Overall, commercial sectors experienced a wide swath of operational impacts due to cyber attacks this year with respondents citing financial losses (38%), reputational damage (36%), and loss of customer or partner relationship (31%) as the most common impacts. However, for the Retail and Hospitality industry specifically, legal fees were the most impactful (35%). These responses emphasize the far reaching ramifications of cybercrime and advanced attacks against cyber-physical systems.

Production shut down	**27%**	Legal implications	**27%**
Product delivery shut down	**30%**	Regulatory implications	**21%**
Financial losses	**38%**	Patient care disruption	**22%**
Loss of intellectual property	**29%**	Human injury	**13%**
Reputational damage	**36%**	Public safety	**18%**
Loss of customer or partner relationship	**31%**	None of the above	**4%**
Staffing changes	**16%**	Other	**13%**

Resilience Strategies are Paying Off in Risk Reduction

When asked about the confidence respondents have in their organization's ability to withstand attacks today versus 12 months ago, most respondents (59%) cited greater confidence in the ability of their organization's CPS — indicating a growing maturity around the defense of CPS environments and a deeper understanding of their impact on critical infrastructure.



Some Security Gaps Still Need to be Addressed

Although many respondents are more confident in their organization's ability to withstand attacks today, there are several capabilities they feel that are still missing from their cybersecurity program. For Commercial Real Estate companies, having an accurate asset inventory was the most important capability they were missing that may have decreased the impact of cyberattacks their organization experienced this year (40%). Retail and Hospitality respondents selected identity and access management (33%), while Data Center industry respondents cited vulnerability management (43%) as the most important security capability they were missing. These security gaps emphasize sector-wide commercial cybersecurity challenges including the need for unique CPS visibility and a dynamic approach to managing exposures.

40%

Commercial Real Estate companies, having an accurate asset inventory was the most important

33%

Retail and Hospitality respondents selected identity and access management

43%

Data Center industry respondents cited vulnerability management

To combat the challenges uncovered by The Global State of CPS Security 2024 Study, organization can implement the following 3 measures to strengthen cybersecurity in their commercial businesses:

1. Gain a comprehensive asset inventory

The foundation of any effective commercial cybersecurity strategy begins with a comprehensive and current inventory of all assets. With full asset visibility into all CPS in your BAS environment, you can understand what assets you have, where they are located, what their status is, and how they function. This begins with an approach that prioritizes non-passive collection methods. Non-passive methods provide deep visibility without the need for hardware or configuration changes and are recommended for commercial environments.

2. Identify, validate, and prioritize exposures relevant to their BAS

With a strong exposure management strategy, commercial companies can systematically identify and prioritize vulnerabilities in order to reduce the likelihood of a security breach. By proactively addressing weaknesses in critical systems, networks, and applications, organizations can reduce the risk of exploitation by threat actors.

3. Extend CPS controls & governance to support all use cases

Once enterprise-wide visibility is achieved and an effective exposure management strategy is in place, commercial companies can extend their CPS security controls to cover network protection, secure access, and threat detection use cases. By partnering with a comprehensive platform that supports the full CPS cybersecurity journey, commercial organizations can more quickly and easily progress in their CPS security and reduce their attack surface.

Learn More

To learn more, download the full report:
The Global State of CPS Security 2024: Business Impact of Disruption

Download

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.