INDUSTRY SNAPSHOT

The Global State of CPS Security 2024: Healthcare

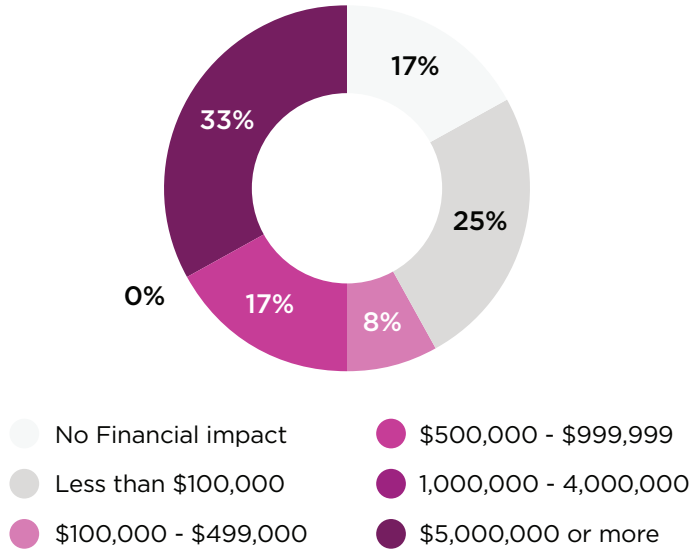
Cybersecurity leaders in the healthcare sector dealt with significant challenges in 2024 when it comes to the protection of cyber-physical systems (CPS) including internet of medical things (IoMT), internet of things (IoT), building management systems (BMS) and operational technology (OT). Frequent and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

To better understand how critical infrastructure 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 76 respondents who work in the healthcare sector:

Cybersecurity Incidents Affecting CPS Result in Steep Financial Losses

When asked about the financial impact of cyberattacks to their organization, nearly 50% of respondents reported a financial loss of $500,000 or more. And, almost 25% reported a loss of $1,000,000 or more. Several factors contributed to these losses, the most common being recovery costs (selected by 41% of respondents), employee overtime (38%), revenue lost (34%), and regulatory fines (32%). These findings highlighted the major financial impacts amid persistent cyber attacks.



Ransomware Still Plays Heavily into Recovery Costs

When asked how much their organization paid in ransom, alarmingly, 78% of respondents met ransomware demands of $500,000 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	**11%**
Less than $100,000	**0%**
$100,000 - $499,000	**11%**
$500,000 - $ 999,999	**39%**
$1,000,000 - $499,999,999	**39%**
$500,000,000 or more	**0%**

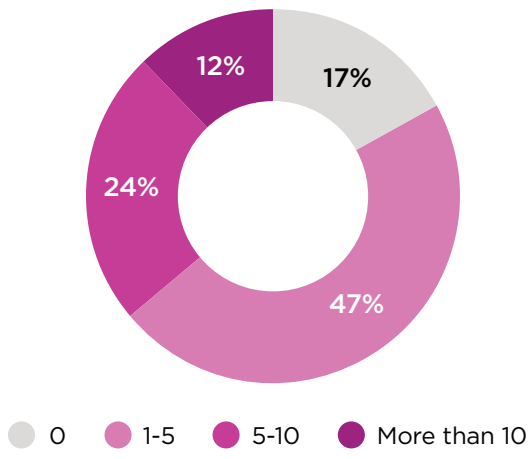
Consequential Operational Impacts Felt by Organizations Worldwide

The healthcare sector experienced a wide swath of operational impacts due to cyber attacks this year with respondents citing financial loss (38%), regulatory implications (34%), product delivery shut down (33%), and patient care disruption (24%) as the most common impacts. These responses emphasize the far reaching ramifications of cybercrime and advanced attacks against cyber-physical systems.

Production shut down	**24%**	Legal implications	**20%**
Product delivery shut down	**33%**	Regulatory implications	**34%**
Financial losses	**38%**	Patient care disruption	**24%**
Loss of intellectual property	**30%**	Human injury	**13%**
Reputational damage	**30%**	Public safety	**22%**
Loss of customer or partner relationship	**29%**	None of the above	**9%**
Staffing changes	**28%**	Other	**17%**

A Remote Access and Supply Chain Problem

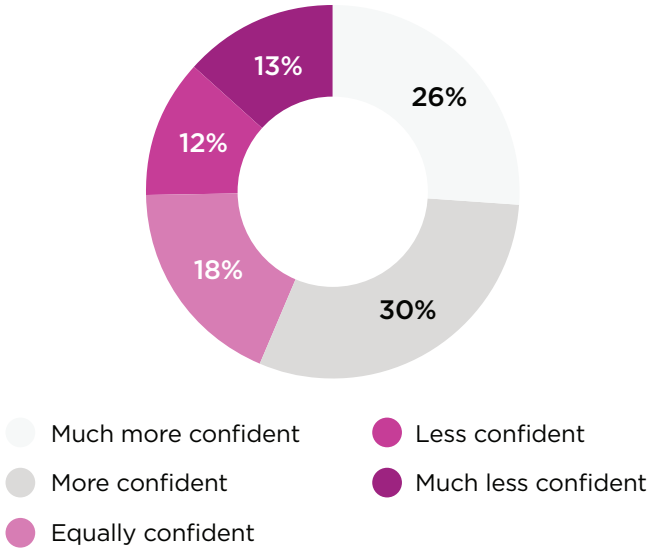
When asked about the origin of cyberattacks that occurred in the last 12 months, 83% of respondents cited that one or more cyber attack – and 35% said five or more attacks – in the past 12 months originated from third-party supplier access to the CPS environment. And yet, over half (63%) admit to having only partial or no understanding of third-party connectivity to the CPS environment.



I have no understanding of third party connectivity	**24%**
I have some understanding of third-party connectivity, but I am concerned about what I don't know	**39%**
I have 100% confidence that I understand all connections to my third-party environment	**37%**

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 (57%) 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.



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.