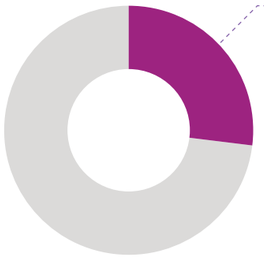
The Global State of CPS Security 2024: Business Impact of Disruptions

CLAROTY

Financial Impacts



27%

Over a quarter (27%) of organizations reported a financial impact of $1 million USD or more from cyber attacks affecting cyber-physical systems

Top three contributing factors:

- Lost Revenue
- Recovery Costs
- Employee Overtime

53%

Met ransom demands of more than $500,000 USD to recover access to encrypted systems and files in order to resume operations.

78%

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

Operational Impacts

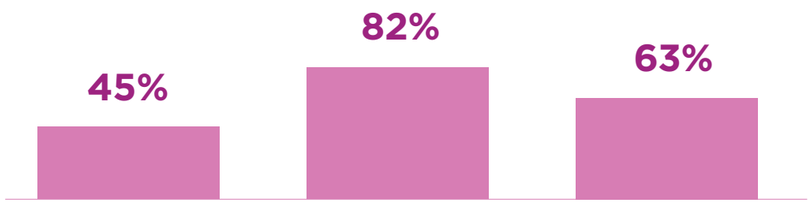
33%

Reported a full day or more of operational downtime

49%

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

Remote and Third Party Access

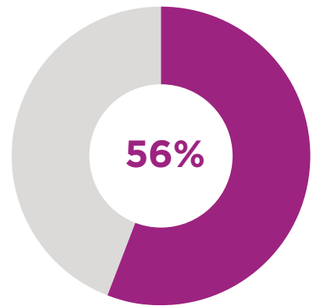


Said at least half of their organization's CPS assets are connected to the internet

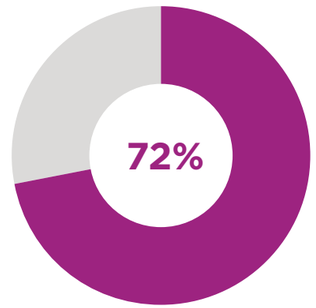
Experienced at least one cyber attack that originated from third-party access to the CPS environment

Have only partial or no understanding of third-party connectivity to the CPS environment

Risk Reduction Efforts



Have greater confidence in the ability of their organization's CPS to withstand cyber attacks today versus 12 months ago



Expect to see quantifiable improvements in their CPS security in the next 12 months