

Cybersecurity incidents grow costlier amid persistent complexity

UII DATA REPORT 185 | SEPTEMBER 2025

SUMMARY

According to the Uptime Institute Data Center Security Survey 2025, the majority of operators have experienced a cyber incident this year. IT software and network configuration issues remain the leading cause of these incidents. Cyber events are also growing more costly — with 2025 marking the first year operators reported the cost of their most impactful incidents as exceeding \$50 million.

Fewer than half of data center operators currently have a dedicated cybersecurity team to handle tasks and procedures.

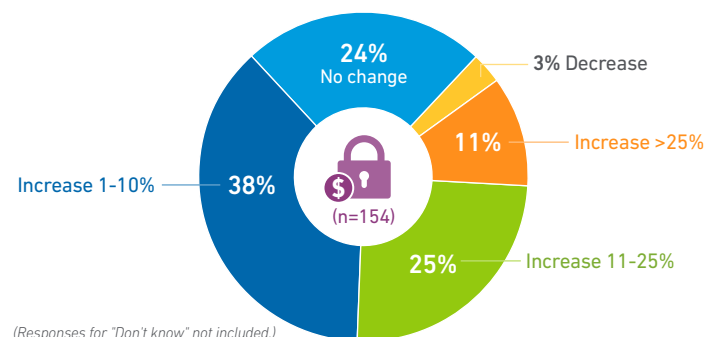
Although most operators believe better training could have prevented their most recent major outage, the growing interconnectedness of data center systems makes it difficult to deliver effective training across siloed teams.

ABOUT THIS SURVEY

The Uptime Institute Data Center Security Survey 2025 was conducted online from June to August 2025, and had over 980 respondents. This report highlights some of the findings.

Most operators say their cyber budget will increase

Do you think your data center cybersecurity spending will increase, decrease, or stay the same for the next 12 months compared with the previous 12 months?

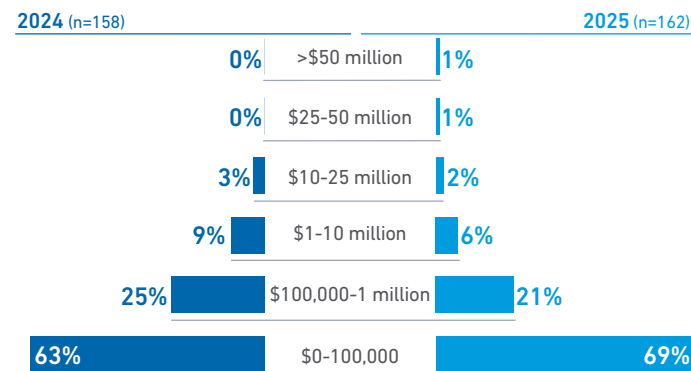


UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Most costly cyber events now exceed \$50 million

Please estimate the total cost of your category 1-5 cybersecurity incident, including direct, opportunity and reputation costs:

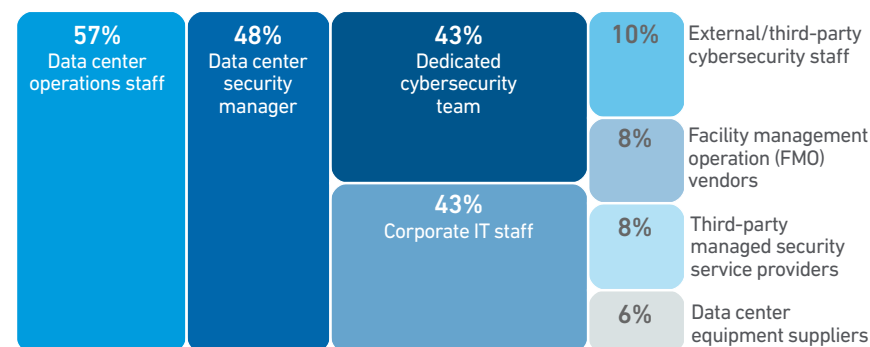


UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Operations staff still perform the bulk of cyber procedures

Which of the following factors are primarily responsible for executing the required tasks and procedures of your data center cybersecurity plans? Choose no more than three. (n=279)



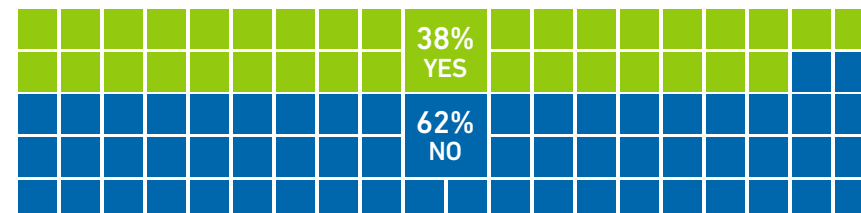
(Responses for "Other" and "Don't know" not included.)

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

More than a third of operators grant third parties private network access

Do any of your organization's vendors/third-party providers access or connect to the internal networks of your data centers? (n=278)



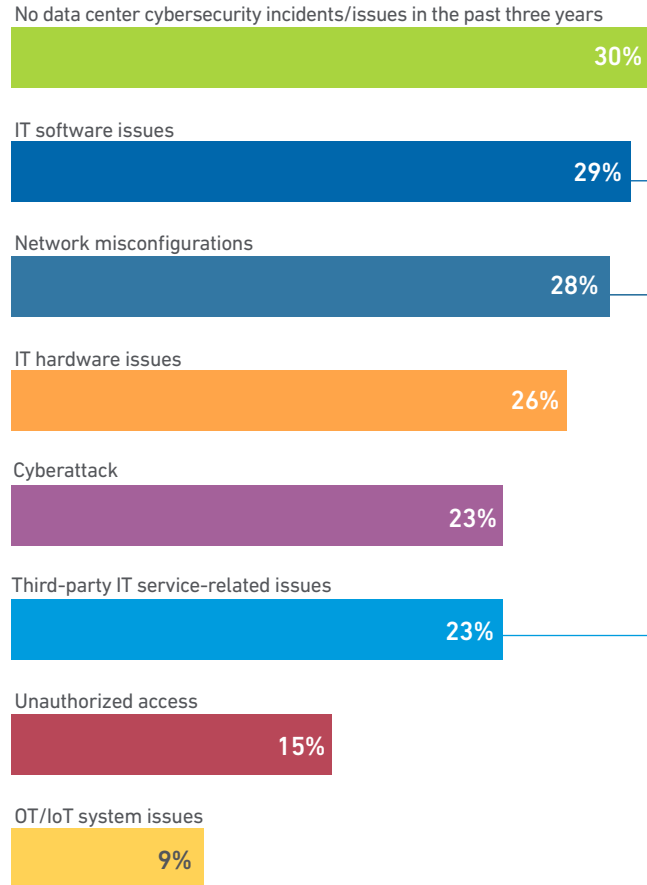
(Responses for "Don't know" not included.)

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Most cyber incidents are rooted in IT software problems

Which of the following have been the most common causes (if any) of data center cybersecurity issues/incidents that have affected your organization over the past three years? Choose no more than three. (n=388)



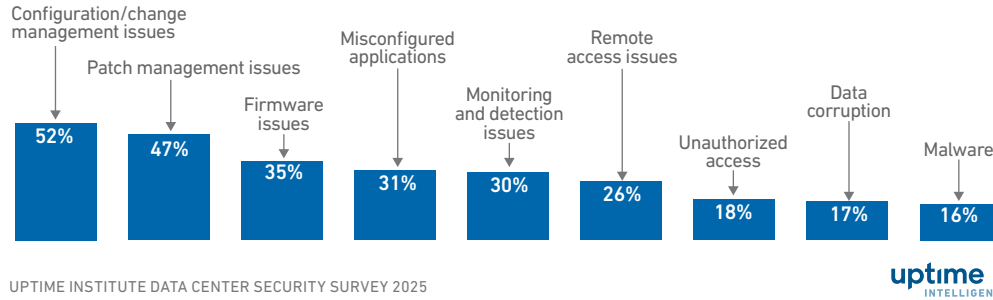
(Responses for "Other" not included.)

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Configuration problems are the leading cause of IT software issues

Which of the following are the most common causes of your cybersecurity-related IT software issues? Choose no more than three. (n=96).

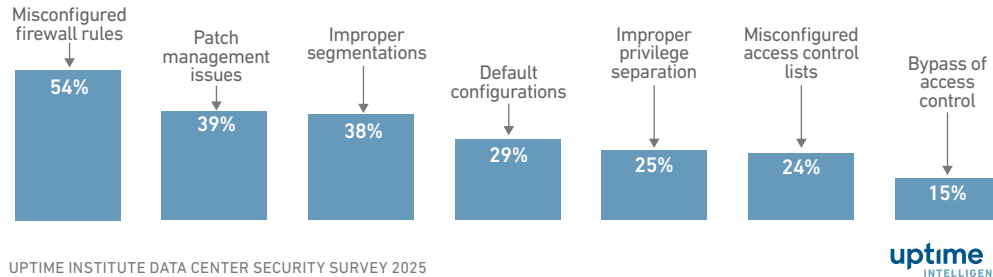


UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Misconfigured firewall rules are the leading cause of network issues

Which of the following are the most common causes of your cybersecurity-related network misconfiguration issues? Choose no more than three. (n=95).

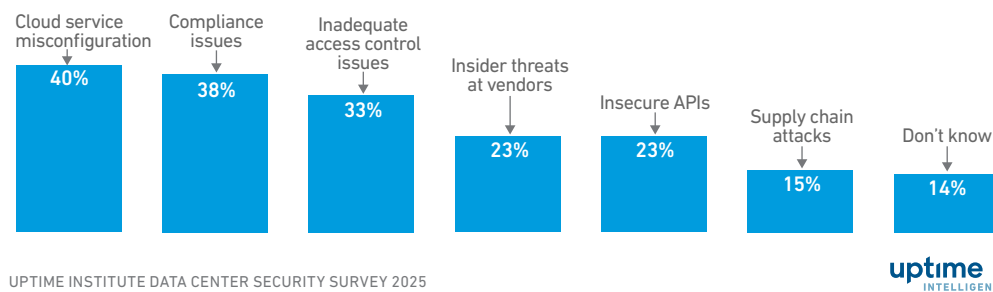


UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

Most third-party incidents stem from cloud misconfigurations

Which of the following are the most common causes of your third-party, cybersecurity-related issues? Choose no more than three (n=78)



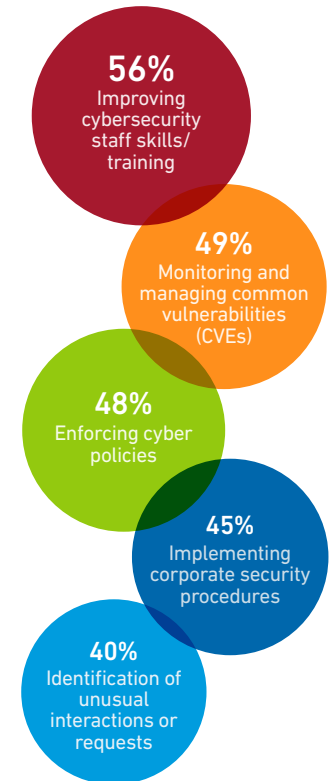
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

uptime
INTELLIGENCE

(All of the above: Responses for "Other" not included.)

Operators say staff training could have prevented incidents

Which of the following processes or procedures would have prevented your most impactful cybersecurity incident? Choose all that apply. (n=162)

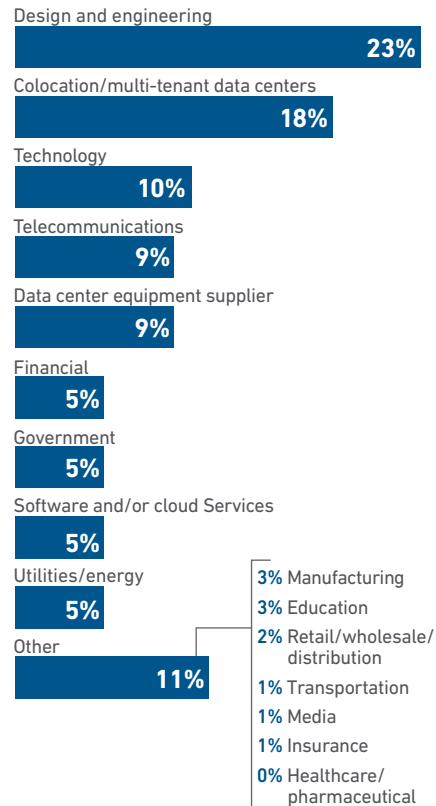


(Only includes respondents who had a Category 1-5 outage.)

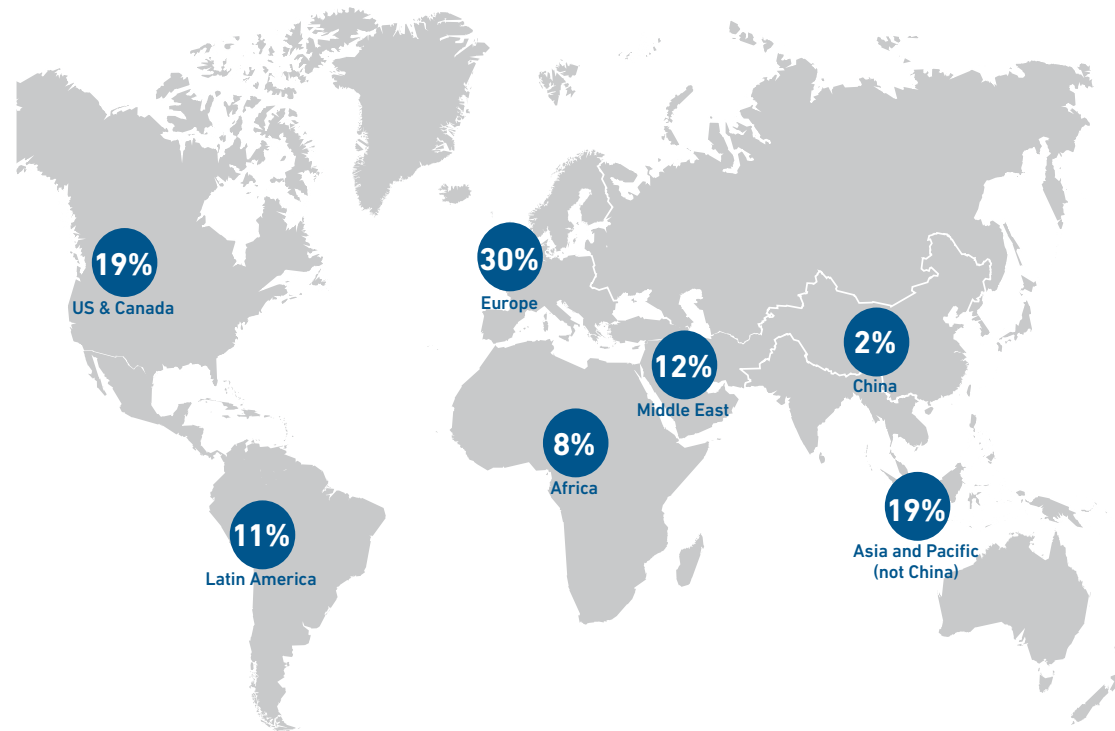
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2025

Demographics: Uptime Institute Data Center Security Survey 2025

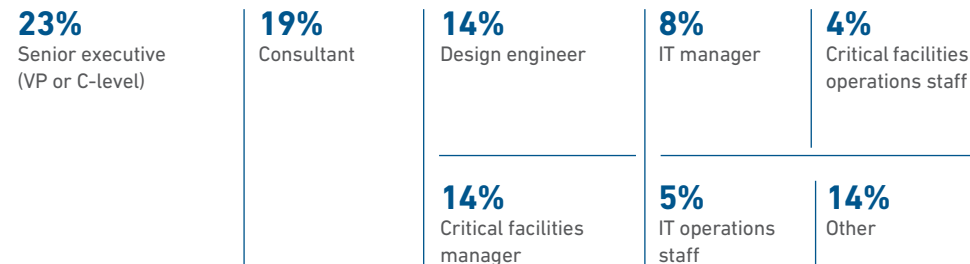
Verticals (n=981)



Company location (n=981)



Digital infrastructure environment (n=641)



Author

Rose Weinschenk, Research Associate
rweinschenk@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers – the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions.

With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.

Uptime Institute is headquartered in New York, NY, with offices in Seattle, London, Sao Paulo, Dubai, Singapore, and Taipei. For more information, please visit www.uptimeinstitute.com

All general queries:

Uptime Institute
405 Lexington Avenue,
9th Floor, New York,
NY 10174, USA
+1 212 505 3030
info@uptimeinstitute.com