uptime INTELLIGENCE

DATA REPORT

Cyber incidents are common — and often significant

Douglas Donnellan, Research Analyst, ddonnellan@uptimeinstitute.com

Cybersecurity is a growing concern for data center operators in 2024. Most have experienced a cybersecurity incident in the past three years, with more than one in three having considerable impact. New technologies and services offered by third parties provide opportunities to integrate IT and OT systems further and improve efficiency. But they can also elevate cyber risks. Results from the Uptime Institute Security Survey 2024 provide insights into how operators are maintaining cyber resiliency to protect the increasingly connected systems used by data centers.

The Uptime Institute Security Survey 2024, conducted online in April and May 2024, had more than 900 respondents. This report highlights some of the findings.

KEY POINTS

- Cybersecurity incidents have become more frequent in 2024, with more than one in three operators rating their impacts as significant, serious or severe.
- Network configuration, IT software and power-related issues are the most common causes of cyber incidents. However, these often relate to change management issues rather than malicious cyberattacks.
- A growing number of operators allow vendors and third parties to access internal data center networks. Although this can be essential for troubleshooting and service delivery, it can also expand the attack surface, often necessitating frameworks such as zero trust architectures to mitigate potential risks.
- Remote control capabilities for IT and OT systems are increasing in 2024. While these can enhance efficiency and monitoring, they also elevate cyber risks, particularly for legacy systems.

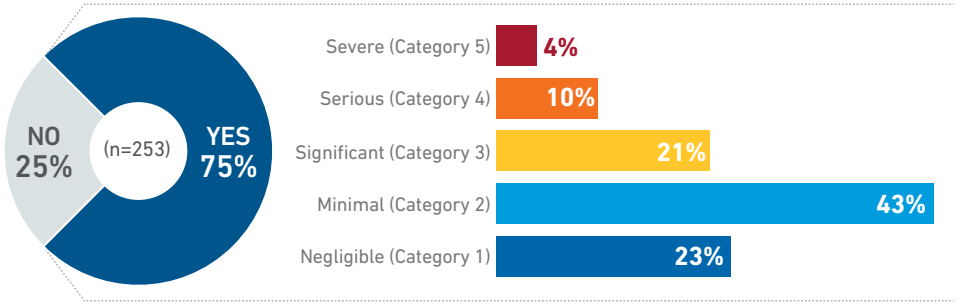
Uptime Intelligence is an independent unit of Uptime Institute dedicated to identifying, analyzing and explaining the trends, technologies, operational practices and changing business models of the mission-critical infrastructure industry. For more about Uptime Institute Intelligence, visit **uptimeinstitute.com/ui-intelligence** or contact **research@uptimeinstitute.com**. Intelligence reports do not represent Uptime Institute's position and do not constitute investment or technical advice.

More than one-third of recent cyber incidents had considerable impact

Cybersecurity incidents, defined as disruptions involving cybersecurity and not necessarily direct attacks, are increasing. Three in four data center operators report experiencing such incidents in the past three years — an 11-percentage point increase from 2023 (see *Network complexity heightens cyber-risks for data centers*). In addition, over one-third rated their most impactful incident in 2024 as significant, serious or severe (see **Figure 1**).This increase in incident frequency can be attributed to the continued rise in network complexity, which expands the attack surface for malicious actors and the growing sophistication of cyber threats. The high impact ratings likely stem from the rising dependence on interconnected IT and OT systems, where disruptions can cause cascading failures. Furthermore, cloud and edge computing integrations expose data centers to more external threats, raising operational risks and incident consequences.

Figure 1

Did your organization experience an impactful cyber incident in the past three years? On a scale of 1 (negligible) to 5 (severe) how would you classify your data center's most impactful cybersecurity incident in the past three years?



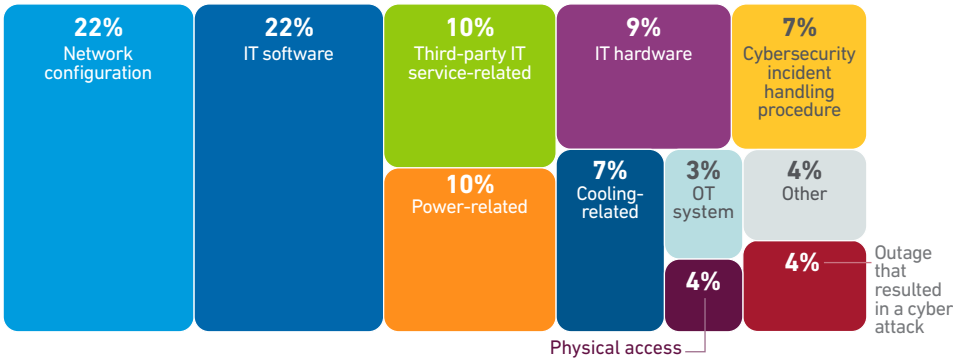
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

Network and software issues cause most impactful cyber incidents

Network configuration and IT software issues are the primary causes behind the most impactful cybersecurity incidents in data centers (**Figure 2**). Most of these incidents, however, are likely linked to change management issues, rather than malicious activity. For example, IT software problems, such as flawed updates, patches or compatibility failures, can compromise system integrity, leading to downtime, lockouts or system failures. Poorly executed changes or overlooked security settings can unintentionally expose sensitive data or restrict access for authorized users, causing significant operational disruptions. Despite advances in cyber risk assessments for data centers, more robust cybersecurity protocols and frameworks are required to mitigate these risks (*Operators boost cybersecurity efforts, but more work is needed*).

Figure 2

What was the primary cause of your most impactful data center cybersecurity incident? (n=162)



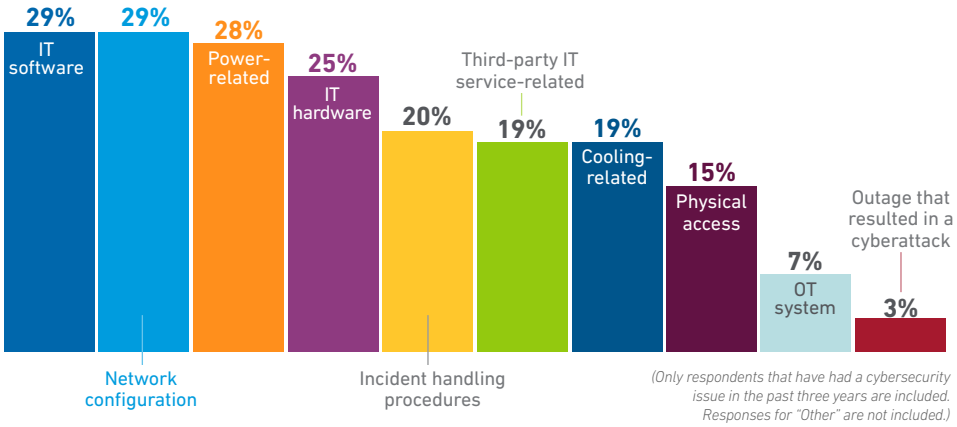
UPTIME INSTITUTE DATA CENTER AND IT SPENDING SURVEY 2024

Software, network and power issues cause most cyber incidents

Software, network and power issues are the leading causes of the most impactful cybersecurity incidents, as well as the most common causes of cyber incidents overall (**Figure 3**). These incidents likely stem from change management issues (discussed in previous section) and are often interrelated. For example, power issues can disrupt software and networking functions. If system configurations are not backed up effectively, cyber defenses may falter — leaving systems vulnerable or inaccessible to authorized users. In severe situations, power outages can interrupt the processes for bringing the data center back online, exacerbating the outage's impact (*Weak security processes can increase the impact of failures*).

Figure 3

Over the past three years, which of the following issues have been the most common cause (if any) of data center cybersecurity issues/incidents that have affected your organization? Choose no more than three. (n=373)



UPTIME INSTITUTE DATA CENTER AND SECURITY SURVEY 2024

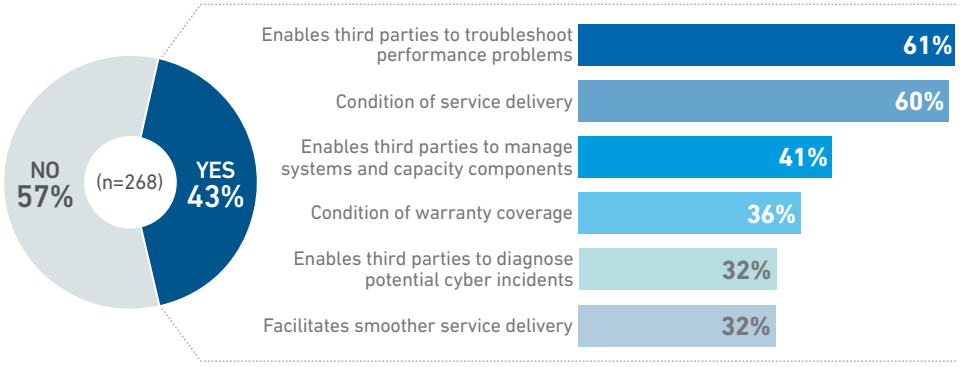
uptime INTELLIGENCE

Third-party access to internal networks is a requirement for some

Nearly half (43%) of operators allow third-party access to internal networks in 2024 (**Figure 4**), an increase from 38% in 2023. The primary reasons cited are to enable troubleshooting and meet service delivery requirements, highlighting the growing dependence on third-party services for managing complex data center environments. For example, seamless integration of hybrid cloud strategies and fast resolution of performance issues may necessitate this access. However, third-party access can also widen the attack surface and increases the risk of potential breaches. Many operators have adopted a zero trust framework to mitigate these risks, which provides tightly controlled and monitored access to specific resources without broadly exposing internal networks.

Figure 4

Do any of your organization's vendors/ third party providers access/connect to the internal networks of your data centers? If so, what are the reasons for allowing access? Choose all that apply.



UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

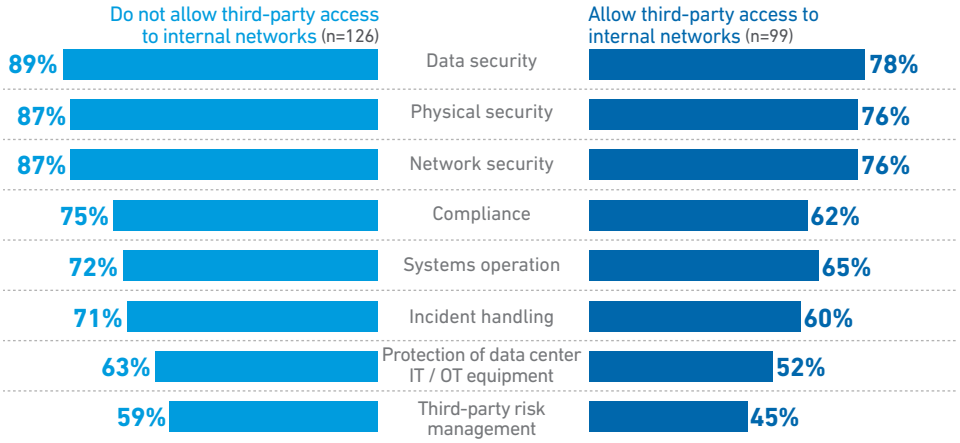
uptime INTELLIGENCE

Assessments vary by those allowing third-party network access

Operators who do not allow third parties to access internal data center networks tend to review more areas as part of their cyber risk assessments than those who do (see **Figure 5**). Those who do not grant network access to third parties were more than 10 percentage points more likely to select nearly every response category. Notably, the most significant disparity (14 percentage points) was in the review of third-party risks. Variations in business models, data sensitivity and industry-specific compliance requirements between the two groups may account for this difference. Additionally, organizations that do not include third-party risk management in their assessments may rely on a comprehensive zero trust framework for external interactions.

Figure 5

Which of the following areas are reviewed by your organization when conducting data center cybersecurity assessments? Choose all that apply. (total n=225)



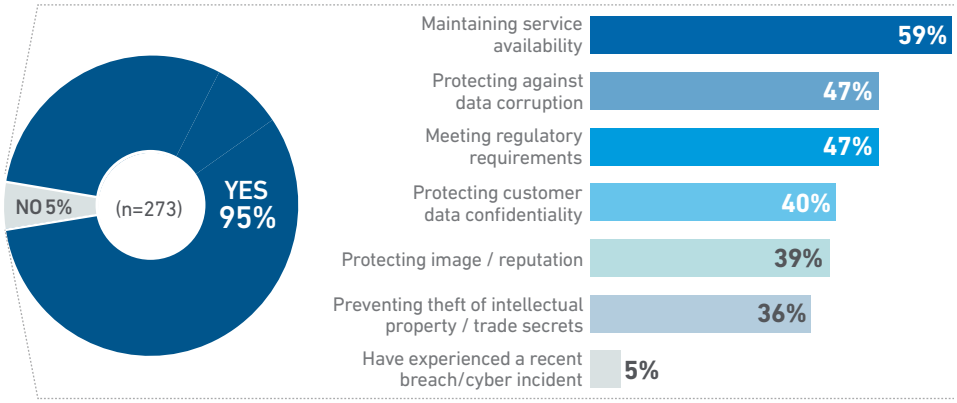
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

Most conduct cyber assessments proactively

Nearly all organizations conduct cybersecurity assessments and most use internal and external resources (**Figure 6**). This approach emphasizes comprehensive evaluation strategies to identify vulnerabilities. Notably, only 5% of respondents cited a recent breach or incident as the reason for conducting an assessment, suggesting that proactive measures are more common than reactive ones. This indicates a strong industry focus on prevention and resiliency, underlining the importance of continuous assessment to mitigate potential risks and maintain trust.

Figure 6

Has your organization had a cybersecurity assessment of its data center IT or OT systems, either internally or by an external company? What are the primary reasons for this assessment? Choose no more than three.



(Only the top six categories, plus those that have experienced a recent breach/cyber incident are included.)

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

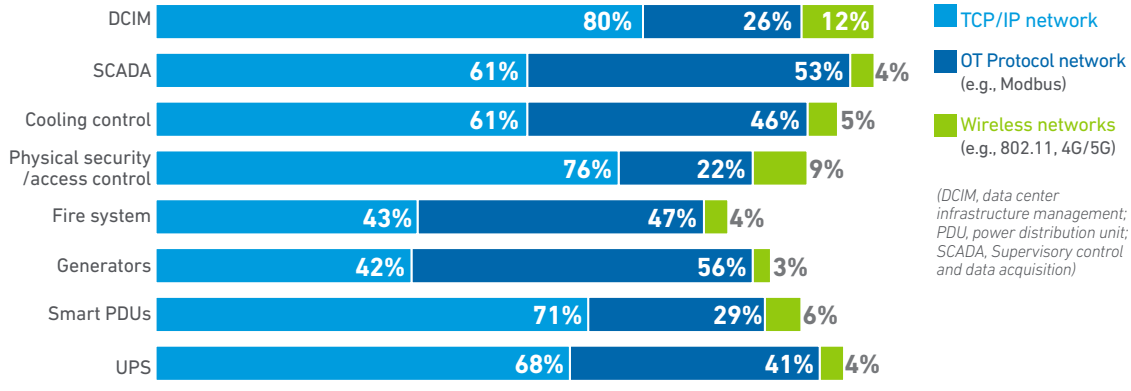
Network approaches for IT and OT systems vary

Most data center operators connect IT and OT systems to TCP/IP networks, which are well-understood from a security standpoint (**Figure 7**). Defense mechanisms, such as firewalls and intrusion detection, make breaches less likely, but these are still vulnerable to distributed denial of service (DDoS) attacks, malware, or ransomware. OT protocol networks have challenges where IT and OT systems converge, especially in legacy facilities where OT protocols, such as Modbus or BACnet, were originally designed for isolated environments. Operators can mitigate these with network segmentation, monitoring, and secure gateways.

Wireless networks are least used for IT and OT systems because they expose systems to remote attacks. While advanced measures (such as WPA3 encryption) can mitigate these risks, they still present significant cyber risks and are often deployed in specific use cases.

Figure 7

Which of the IT and OT systems used to operate your data center(s) are connected to a TCP/IP network, OT protocol network, or wireless networks? Choose all that apply. (n=294)



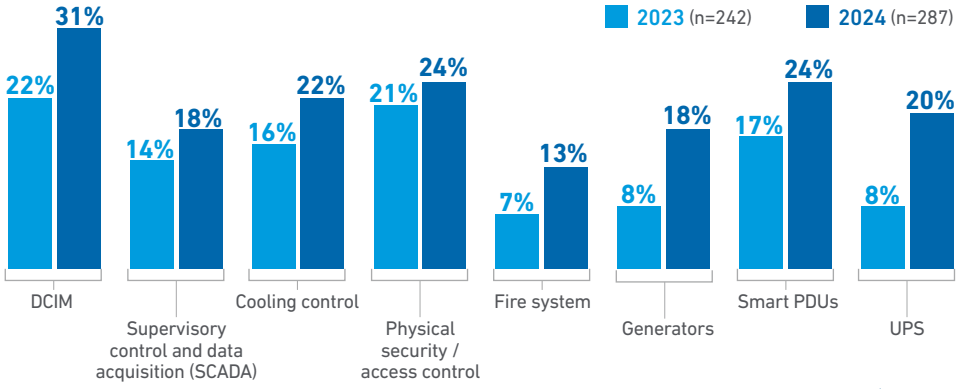
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

Remote control capabilities are increasing for IT and OT systems

In 2024, more IT and OT systems used by data center operators provide remote control capabilities compared with 2023 (see **Figure 8**). This shift aligns with the growing adoption of technologies that improve operational efficiency, visibility, and predictive capabilities. Systems such as DCIM, physical security/access control and smart PDUs are notably prominent and provide real-time data and aid in streamlining and monitoring operations. However, integrating these systems heightens cyber risk, particularly with OT systems, which often focus on reliability rather than security. This can pose significant challenges, especially for legacy sites that find it difficult to implement security measures that match the increased complexity of their infrastructure.

Figure 8

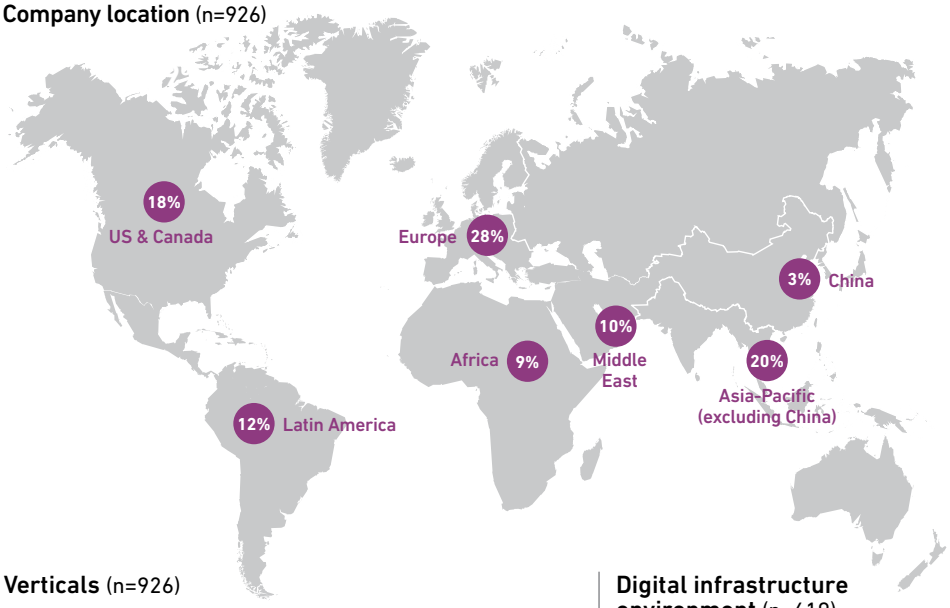
Which of the IT and OT systems used to operate your data center(s) provide remote (offsite) control capabilities? Choose all that apply.



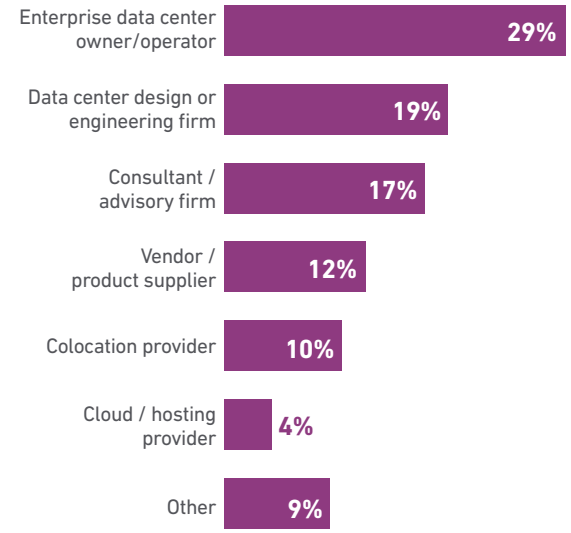
UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

Demographics:
Uptime Institute Data Center Security Survey 2024

Company location (n=926)



Verticals (n=926)



Digital infrastructure environment (n=619)

19% Senior executive (VP or C-level)	**19%** Consultant
15% Design engineer	**14%** Critical facilities manager
12% IT manager	**6%** Critical facilities operations staff
6% IT operations staff	**10%** Other

UPTIME INSTITUTE DATA CENTER SECURITY SURVEY 2024

uptime INTELLIGENCE

All general queries

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