THALES
Building a future we can all trust

#2025DataThreatReport

2025

Critical Infrastructure DATA THREAT REPORT

AI, Quantum and the Evolving Data Threatscape

cpl.thalesgroup.com

Introduction

Critical infrastructure (CI) organizations, which include those involved in energy and utilities, telecommunications and transportation, play a broad array of roles across the economic spectrum. Because they work with a high concentration of sensitive and high-value data — and outages can range from an inconvenience to a wide-scale disaster — these firms are heavily regulated, and the information and systems they steward are major targets for cybercriminals. Top challenges for these organizations include a rapidly evolving threat landscape, malware, ransomware, phishing, compliance mandates and third-party risks.

In this executive summary, we share key findings from the **2025 Thales Data Threat Report** focused on CI organizations and examine differences between CI survey respondents and global responses across all industry verticals. Many of the CI Data Threat Report survey results are similar to overall responses, but we note key differences.

S&P Global
Market Intelligence

Source: 2025 Data Threat Report custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

Sponsored by

ARROW
Five Years Out

EXCLUSIVE NETWORKS

CLIMB

TD SYNNEX

Note: All charts displayed in this document are from S&P Global Market Intelligence 451 Research's 2021-2025 Data Threat custom surveys.

Key Findings

Trends in Data Security

Half of CI organizations' data stored in the cloud is sensitive, and yet many fall short of leveraging basic data security controls:

22% of CI respondents have little or no confidence in identifying where their data is stored.

Only 2% of CI organizations have encrypted 80% or more of their sensitive cloud data key distribution; one-fourth the surveywide results.

CI organizations on average report that 50% of the data they store in the cloud is sensitive.

Tracking AI Development

CI organizations, like those in virtually all industries, are deploying advanced AI systems to remain competitive and improve employee productivity. Ensuring that these systems are secure is a priority:

73% cited the fast-moving AI ecosystem as their top concern, followed by concerns about lack of integrity in models or data (64%) and lack of trust (53%).

74% of CI respondents are investing in GenAI-specific security tools, close to the surveywide result, and 19% are using newly allocated budget.

Right on 'Q'

CI respondents are concerned about the risk of future encryption compromise and quantum computing security threats:

63% are concerned about key distribution, compared to 61% surveywide.

62% have concerns about future encryption compromise, compared to 63% surveywide.

60% are concerned about future decryption of today's data, including harvest now, decrypt later, compared to 58% surveywide.

Cloud Platform Growth and Challenges Continue

CI organizations continued growing their cloud estates, according to findings in the 2025 Data Threat Report, and security remains a top concern:

2.1 The average number of IaaS providers increased slightly from 2.0 in the 2024 survey.

102 The average quantity of SaaS applications in use grew from 83 last year to 102 this year, higher than the survey average of 85 — a 23% increase in just one year.

IaaS/PaaS cloud security (33%) is the top security spending category for CI organizations, followed by security for AI (29%) and identity and access management (29%).

Data Security Fuels Digital Sovereignty

Digital sovereignty remains a key concern of CI organizations, which are increasingly using data security to satisfy compliance requirements:

52% of CI organizations were driven to pursue digital sovereignty by specific customer, regional or global privacy mandates.

50% said that encryption and key management provide sufficient protection to achieve sovereignty objectives.

Identity and Access

75% of respondents indicated that MFA is used by 40% or more of employees, a 63-point increase for CI organizations since 2021.

Application Security: Essential for Data Protection

39% of CI organizations use more than 500 APIs; 20% use more than 1,000 (compared to 34% and 16%, respectively, surveywide).

58% of CI respondents said code vulnerabilities are a major concern for application security, placing it as the top response, similar to 59% surveywide.

Critical Infrastructure Observations

Structural and geopolitical changes in 2025 will likely prompt enterprises to rethink their security strategies. The CI Data Threat Report results suggest that organizations would be wise to focus on their most valuable asset: the data they collect, process, store and steward for stakeholders and customers. One sign of improvement is that the number of CI organizations experiencing a recent data breach has decreased. In 2021, 37% of CI organizations had experienced a breach in the prior 12 months; this number dropped to 15% in the 2025 survey — a significant 22 percentage point decrease, similar to the surveywide reduction from 41% in 2021 to 14% in 2025.

In 2021, 37% of CI organizations had experienced a breach in the prior 12 months, but this number dropped to 15% in the 2025 survey — a significant 22-point decrease.

CI organizations reported misconfigurations or human error, exploitation of known vulnerabilities, and identity failure or compromise as the top three breach root causes. The top three types of cloud management infrastructure attacks in which CI respondents reported an increase were credential theft/compromise including misappropriated secrets, third-party vulnerabilities and malware injection (e.g., malicious cloud service module).

From Cloud DevOps to Platform Engineering

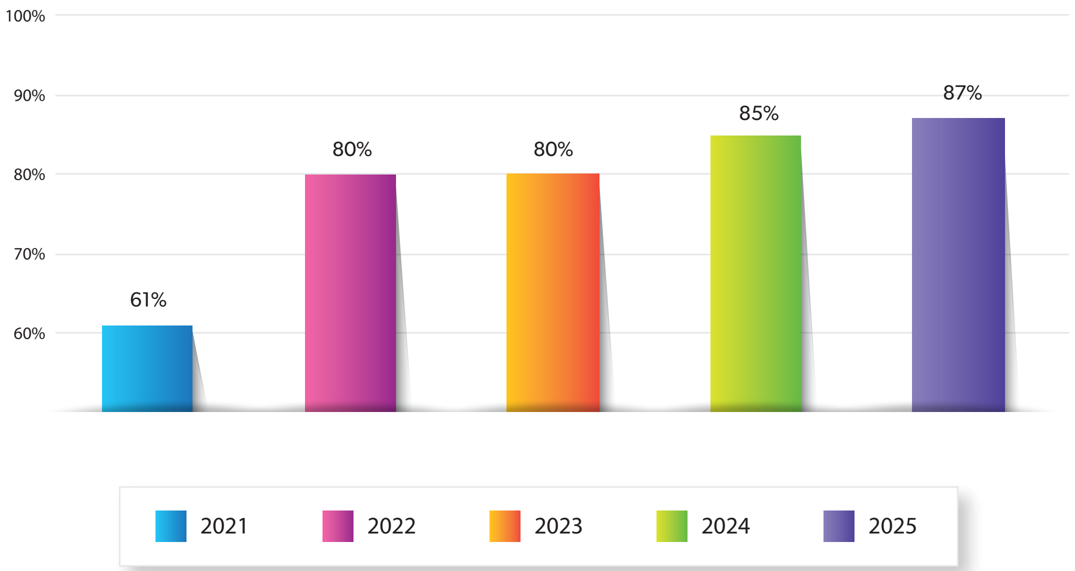
61% **ranked secrets management as a leading DevOps security challenge, compared with 55% across all industries.**

Only 18% **of CI respondents identified secrets management as one of the three most effective technologies in protecting data, despite the devastating impact of compromised secrets, just higher than 16% surveywide.**

Data Security

Understanding data is critical to securing it effectively, and there are encouraging results in data classification: 87% of CI respondents reported that they can classify at least half of their data, a notable increase from previous years and similar to surveywide results. The consistency and effectiveness of data discovery and data classification are less clear. Two-thirds (66%) of CI organizations use five or more tools for data discovery and classification, which can lead to misalignment and conflicting protection policies. This misalignment might be contributing to the result that just 2% of CI organizations have encrypted 80% or more of their sensitive data in the cloud — just one-fourth the rate of the overall survey population, and particularly low given the sensitivity of data involved. The 2025 Data Threat Report results show some progress in key areas of data security, but much work remains as organizations mature their data security controls.

Proportion of Critical Infrastructure respondents able to classify at least half of organizational data



Quantum Cryptography

There is better alignment regarding post-quantum cryptography risks in 2025, with 58% of CI respondents prototyping or evaluating new PQC algorithms, similar to the overall result. Deployment timelines are crucial, but early signs of this transition are promising. Regulatory focus on cryptographic protections is also notable: When asked about data sovereignty concerns, nearly one in five CI respondents (17%) said they are using or will use encryption to meet sovereignty mandates.

Application Security

The complexity of application architectures is a key concern, necessitating improved application security. Two-fifths (39%) of CI respondents reported having more than 500 application programming interfaces (APIs) in use (20% have over 1,000), slightly higher than the surveywide result. This proliferation raises broad concerns about vulnerabilities in code and in the software supply chain. While shift-left security controls are the top-cited priority for application protections, CI respondents also emphasized foundational production controls such as dynamic application security testing, API security tools and web application firewalls. Other application security concerns on the architecture side include secrets management, which leads among DevOps security concerns. However, only 9% of CI respondents identified secrets management as the single most effective technology for data protection, and only 18% ranked it in the top three, similar to overall survey results, despite the high risk associated with secrets management failures, which can expose authentication data such as API keys. This concern is amplified given the high reported number of APIs in use.

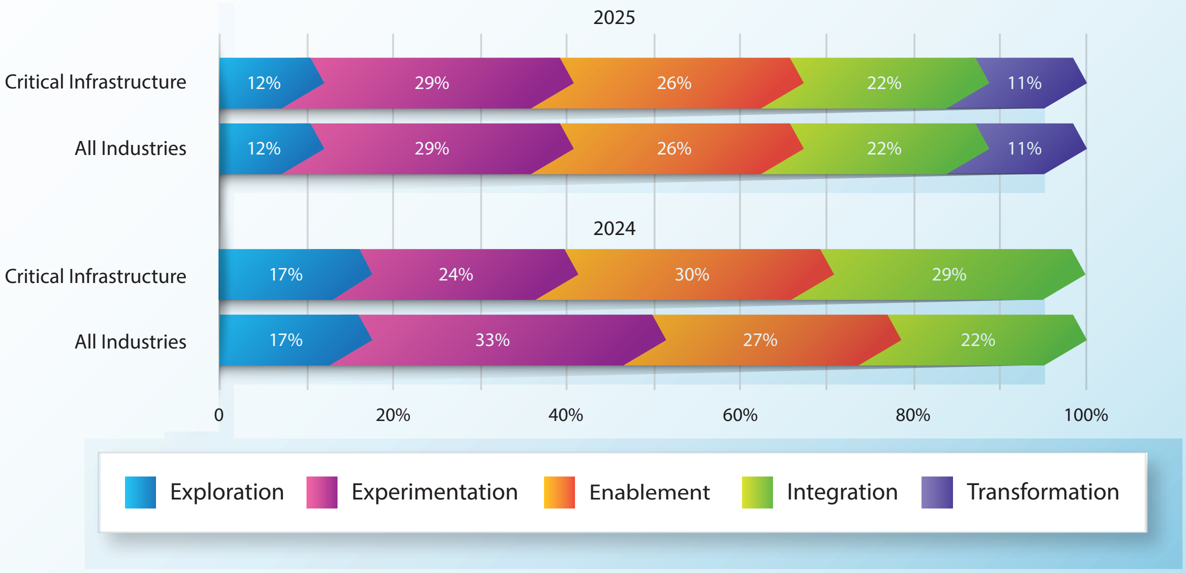
39% of CI respondents reported having over 500 APIs in use and 20% have over 1,000.

Generative AI: Data Takes Center Stage

GenAI poses challenges to data security, but organizations can also use it to respond to security challenges. Increased GenAI integration reflects developing organizational maturity and progress beyond experimentation. An expanded and refined definition of GenAI among respondents reveals expectations for the transformational nature of GenAI as organizations continue their journey toward greater digital maturity.

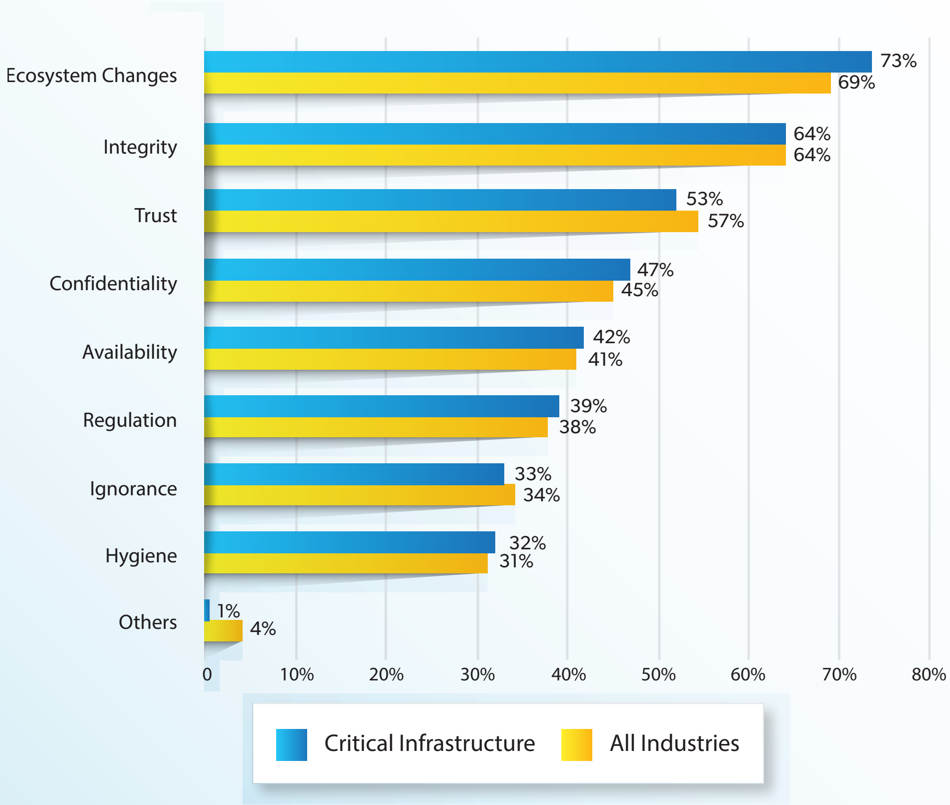
Organizations are under immense pressure to deliver GenAI capabilities, and CI organizations are picking up the pace of adoption. In 2024, CI organizations were slightly behind the general market in terms of AI deployment, trailing by 4 percentage points in enabling employees to use AI and by 1 point in integrating AI into business processes. In 2025, CI organizations are even with surveywide results in all five adoption phases. 74% of CI organizations are investing in AI-specific security tools and services, similar to the surveywide result. Just over half of that spending (55%) comes from existing budgets, and 19% is via newly allocated budget, indicating that AI security is a high concern for these organizations. GenAI's impact may further influence evolving data and privacy regulations, emphasizing the importance of maintaining confidentiality, trustworthiness and safety.

Stages of AI journey



Concerns about the risks of deploying AI are also growing. The top concern is ecosystem and operational alterations forcing rapid changes to existing plans, followed by concerns about model integrity and the trustworthiness of third-party systems. While GenAI is intensifying the focus on data security, hasty implementations raise the risk of data breaches. Vulnerabilities in the DeepSeek GenAI model reported shortly after its V3 release serve as a cautionary tale for security teams. Because GenAI architectures are new for most security teams, prioritizing data security efforts is crucial.

Most concerning GenAI security risks



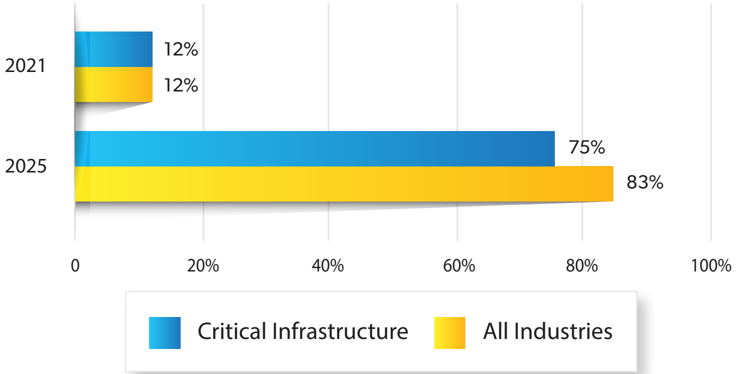
Conclusion

While many of the Data Threat Report results for CI organizations were similar to surveywide responses, key differences emerged. While CI organizations are not adopting technological innovations like AI as aggressively as those in financial services, the addition of generative and agentic AI to a foundation of mature machine learning techniques is a clear priority, with these technologies being widely deployed to aid in employee productivity and transform business processes. Securing AI systems remains a priority for organizations that are concerned about the fast-moving ecosystem and lack of integrity and trustworthiness. This is also reflected in the fact that CI organizations are directing more of their budgets toward AI, with a high percentage of respondents investing in GenAI-specific security tools, using both existing and newly allocated budget.

Continual increases in technical complexity are the result of accelerated digital transformation, and a key indicator is the quantity of APIs in use. CI organizations use many APIs, reinforcing the need for application testing across the life cycle and concerns about software supply chain security. Another area of concern for organizations is secrets management, the leading DevOps security challenge.

Post-quantum cryptography continues to be a source of concern; specifically, CI organizations cited key distribution, future encryption compromise and future decryption of today's data as focus areas. These are only partially being solved by assessing current encryption strategies and prototyping or evaluating PQC algorithms. On a positive note, breach statistics continue to improve, with CI firms reporting a 22-percentage-point drop in recent data breaches since 2021, and while a 63 percentage point increase in the proportion of organizations implementing MFA for more than 40% of employees is encouraging, CI organizations still lag 8 percentage points behind the surveywide result for MFA adoption (75% versus 83%), so more work remains to be done.

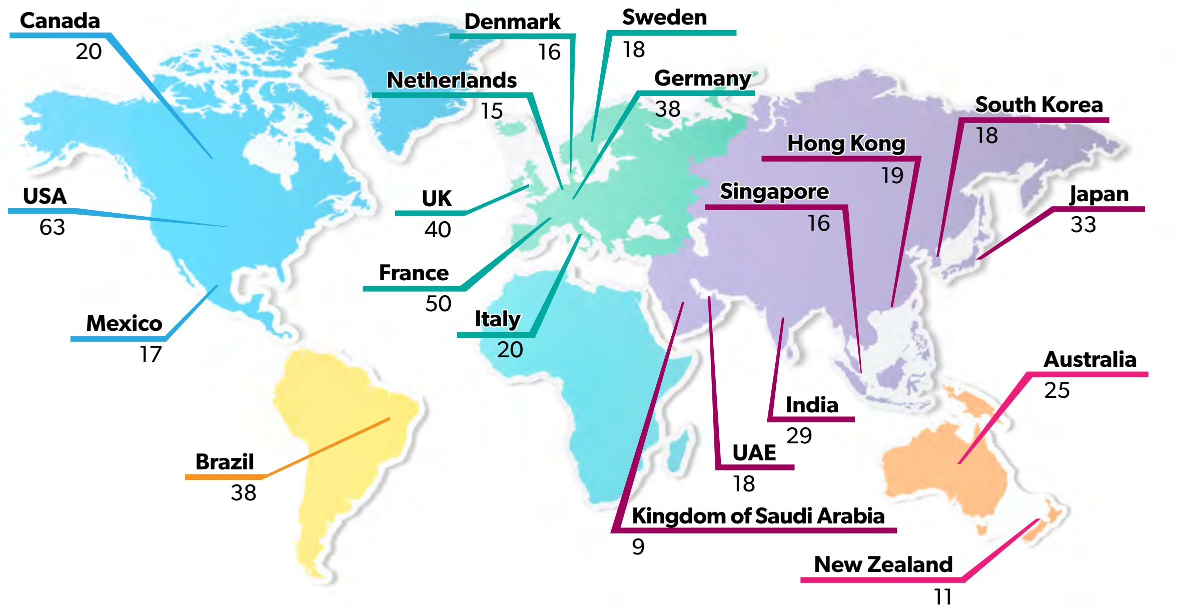
Organizations with 40% or more of employees using Multi-Factor Authentication



While this year's survey results indicate improvements in security posture, much more is needed to elevate operational data security to fully support the capabilities of emerging technologies such as GenAI and to pave the way for future innovations.

About this Study

This research was based on a segment of 513 critical infrastructure respondents extracted from a global survey of 3,163 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million and with US$100 million - $250 million in selected countries. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	23
$250m to $499.9m	103
$500m to $749.9m	123
$750m to $999.9m	130
$1 Bn to $1.49 Bn	45
$1.5 Bn to $1.99 Bn	19
$2 Bn or more	70
Total	513

Industry Sector	Number of Respondents
Energy & Utilities	198
Transportation	187
Telecommunications	128
Total	513

THALES

Building a future we can all trust

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/critical-infrastructure-data-threat-report