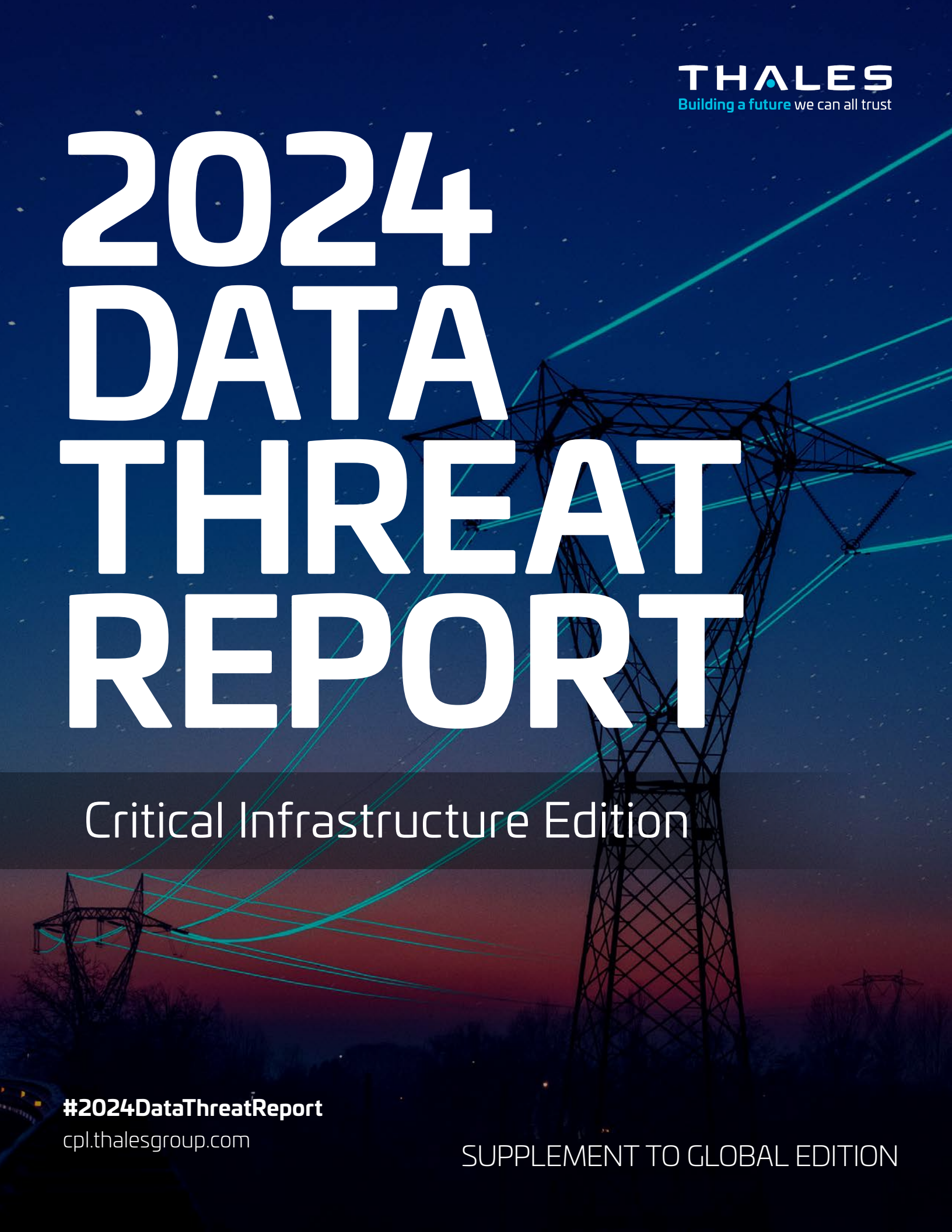


THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Critical Infrastructure Edition

#2024DataThreatReport

cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

Critical infrastructure (CI) — which we define as energy and utilities, telecommunications, transportation, and trucking/shipping enterprises — represents a major segment of the world economy. Successful cyberattacks against organizations in these industries represent significant risks to national security, economic prosperity, and public health and safety. In response, governments worldwide have taken notice of threats to their critical infrastructure and have issued multiple cyber-resilience-related regulations to address the problem, such as the European Union's Network and Information Security directive 2 (NIS 2) and the United States Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

In this paper, we share key findings from the 2024 Thales Data Threat Report (DTR) focused on critical infrastructure organizations, examining the differences between critical infrastructure survey respondents and overall global responses across all industry verticals. Unsurprisingly, many of the critical infrastructure DTR survey results were similar to overall responses, but we do note some key differences.

S&P Global Market Intelligence

Source: 2024 Data Threat Report custom survey from S&P Global Market Intelligence, commissioned by Thales.

Key Findings

Data Breach Trends and Threats

The proportion of CI organizations that have ever been breached remains high, yet 7 percentage points lower than the general survey figure (42% for CI, 49% overall). Encouragingly, recent CI breach history (in the last 12 months) decreased from 22% in 2021 to 15% in 2024, similar to overall decreases.

42%

Ransomware attacks against CI organizations continue growing, with 24% reporting that they have experienced an attack. This is 4 percentage points lower than overall, yet still an increase of 4 percentage points since the previous DTR Critical Infrastructure Edition report in 2022. Planning is still poor, with only about one in seven (15%) CI respondents saying they would follow a formal plan in the event of an attack, 5 points lower than all respondents.

24%

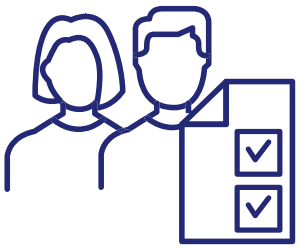
Among CI organizations, human error was the leading cause of cloud-based data breaches at 34% (4 percentage points higher than overall). Failure to apply multi-factor authentication (MFA) to privileged accounts was another major cause, at 20%, 6 percentage points higher than all respondents. **CI organizations continue to struggle with human error and MFA failures at rates higher than the overall population.**

34%

Identity Complexities and Compromise

On average, one-sixth (16%) of all external CI organizational access comes from customers. This figure is identical for overall respondents.

16%



Among survey respondents who cited external identity as an emerging security concern, achieving across workforce and non-workforce identities is one of the top challenges, cited by 61% of both CI and overall respondents.

61%

Increasing DevOps Challenges

56%

Among respondents who cited cloud/DevSecOps security as an emerging security concern, **the greatest proportion cited secrets management (57% overall, 56% CI) as a top DevOps challenge,** followed by workforce IAM issues such as privileged user management (50% overall, 53% CI).

Operational complexity remains a security concern, with 57% of CI respondents reporting they use five or more key management systems, up slightly from 2022 (55%), while the percentage of CI enterprises saying they have 50 or more SaaS apps in use showed a smaller uptick, from 33% in 2022 to 34% this year. These results show a stabilization of hybrid IT complexity, but more simplification is needed.

5+

Risks to Emerging Technologies

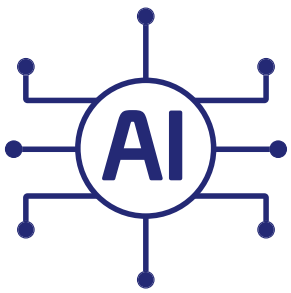
Regarding threats from quantum computing, future compromise of classical encryption techniques, enabling "harvest now, decrypt later" (HNDL) attacks, is leading interest in post-quantum cryptography (69% in CI, 71% overall).

69%

Among CI respondents who identified post-quantum cryptography as an emerging security threat, 49% would likely create resilience contingency plans, and 48% would prototype or evaluate PQC algorithms in the next 18-24 months. **While CI organizations are roughly as concerned about HNDL attacks as the overall population, they are evaluating multiple methods to address those concerns.**

The AI boom is underway: 26% of CI respondent organizations plan to integrate AI into their core products and services in the next 12 months, similar to 27% of overall respondents. Twenty-nine percent of CI organizations are experimenting with AI, compared to 33% of all respondents. **Despite their inherent criticality to the worldwide economy, CI enterprises are embracing innovations in AI.** Yet managing the associated fast changing environmental risks is their greatest concern. Sixty-nine percent of CI respondents said that ecosystem and operational alterations are their greatest, most concerning risks.

26%



Enterprise Observations

This year's DTR provides additional insights into the current enterprise IT and security organization. The need for data security as a discipline remains diffused throughout the enterprise. Functions such as compliance, go-to-market, supply chain and design all incorporate data security.

Security and compliance initiatives are converging as the two areas come together on inputs, processes and outcomes. New cyber-resilience regulations and updates to existing standards including ISO 27000 are specific about what controls organizations need to implement, which is forcing better alignment between security and compliance teams.

KEY STATISTIC

In 2024, of Critical Infrastructure respondents whose organizations failed a compliance audit, 84% reported having some breach history.

84%

KEY STATISTIC

In contrast, for those that passed compliance audits, only 17% have a breach history and only 2% suffered a breach in the last 12 months.

17%

Through the years, DTR findings have shown a strong correlation between compliance achievement and reduced breaches. In the 2024 survey, of the CI respondents whose organizations failed a compliance audit in the last 12 months, 84% reported having experienced some breach in their history (identical to overall respondents). In contrast, for those CI organizations that have not failed a compliance audit only 17% have any breach history, with just 2% having a breach in the last 12 months.

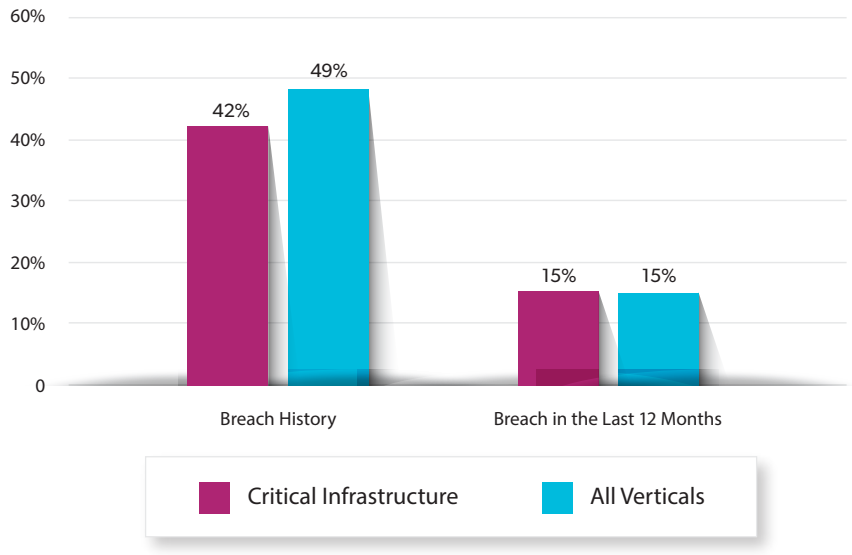
The Threat Landscape

In CI organizations, as in the rest of the world, the attack landscape remains vast and growing. **Nearly nine out of 10 CI respondents (93%) said they experienced an increase in attacks.** The top three fastest-growing types of threats reported by CI organizations were malware, phishing and ransomware. Compared with the 2022 CI survey, malware retained first place, while phishing moved up to second and ransomware slipped to third.

Meanwhile, the most common root causes of cloud-based data breaches for CI organizations were human error (34%), exploitation of a known vulnerability (31%) and failure to use MFA for privileged user accounts (20%). When we examined the root cause of attacks by attacker type, misconfiguration (human error) was ranked as the top root cause for external attackers with financial motivations, geopolitical goals and other ideological goals. Malicious insiders and accidental (human error) attacks exploited known vulnerabilities. Human error can be mitigated in part through deployment of MFA and by maintaining audit logs when used in conjunction with an access management solution.

Among CI respondents, 73% cited MFA as a technology they have chosen to secure access to data in the cloud (on par with the overall average of 74%). This is encouraging, but organizations must ensure they are utilizing strong MFA, such as hardware tokens and phishing-resistant MFA (PKI and/or FIDO passkeys) instead of SMS or email challenges.

Overall Breach History and Recent Breach History



Source: S&P Global Market Intelligence's 2024 Data Threat custom surveys

Ransomware response remains a challenge. For the last three years, fewer than 50% of overall respondents across all verticals and company sizes reported having a formal ransomware plan in place — and only 15% of CI respondents have one. Among CI respondents that have resolved a past ransomware attack, 11% did so by paying a ransom, while 8% of CI organizations said they would pay a ransom to resolve a future attack. Initial breach response is increasingly led by legal teams interfacing with regulators or law enforcement.

More than two-thirds (69%) of CI respondents cited future encryption compromise as the top concern among security threats related to quantum computing, just 2 points below the overall average. Half of CI respondents said they will create resilience contingency plans to satisfy quantum computing security concerns in the next 18-24 months, 11 points higher than the survey-wide result.

The complexity of cloud resources present among end-users, operators and developers continues to grow. Curiously, the percentage of CI enterprises saying they have 50 or more SaaS apps in use remained essentially flat at 34% in the 2024 survey, compared with 33% in 2022. Based on a weighted calculation, CI respondent organizations on average have approximately 90 SaaS apps in use. The percentage of CI enterprises that agree or strongly agree that managing security in the cloud is more complex than managing security on premises has also remained steady (50% in 2022, 51% in 2024).

KEY STATISTIC

Fewer than 50% of overall respondents across all verticals and company sizes reported having a formal ransomware plan in place — and only 15% of CI respondents have one.

15%

Access Control

There is a bit of a sea change underway in terms of how access control is managed — and by whom. **Almost half (49%) of CI respondents in the latest survey agree that organizations should maintain control over their access security**, compared with 58% in the 2022 survey, likely indicating that organizations are increasingly using external providers for access security. Moreover, 43% of CI respondents believe that access security solutions should be delivered by an agnostic security provider rather than a cloud service provider — in line with the 2022 survey (42%) — while 39% agree that an agnostic access management solution can best protect multicloud environments.

KEY STATISTIC

To achieve zero-trust security, 36% of CI respondents agree that access management and authentication plays a key role, especially with averaging more than 50 SaaS apps to manage.

36%

In terms of achieving zero-trust security, 36% of CI respondents agree that access management and authentication plays a key role. Having more than 50 SaaS apps necessitates a deeper dive into authentication journeys. CI organizations have a highly disparate user base, ranging from corporate staff to factory floor workers and field engineers, and enabling zero-trust with the plethora of SaaS apps and disparate users requires flexible access policies. Similarly, for air-gapped environments, an on premises authentication solution is needed to protect resources.

Next Steps

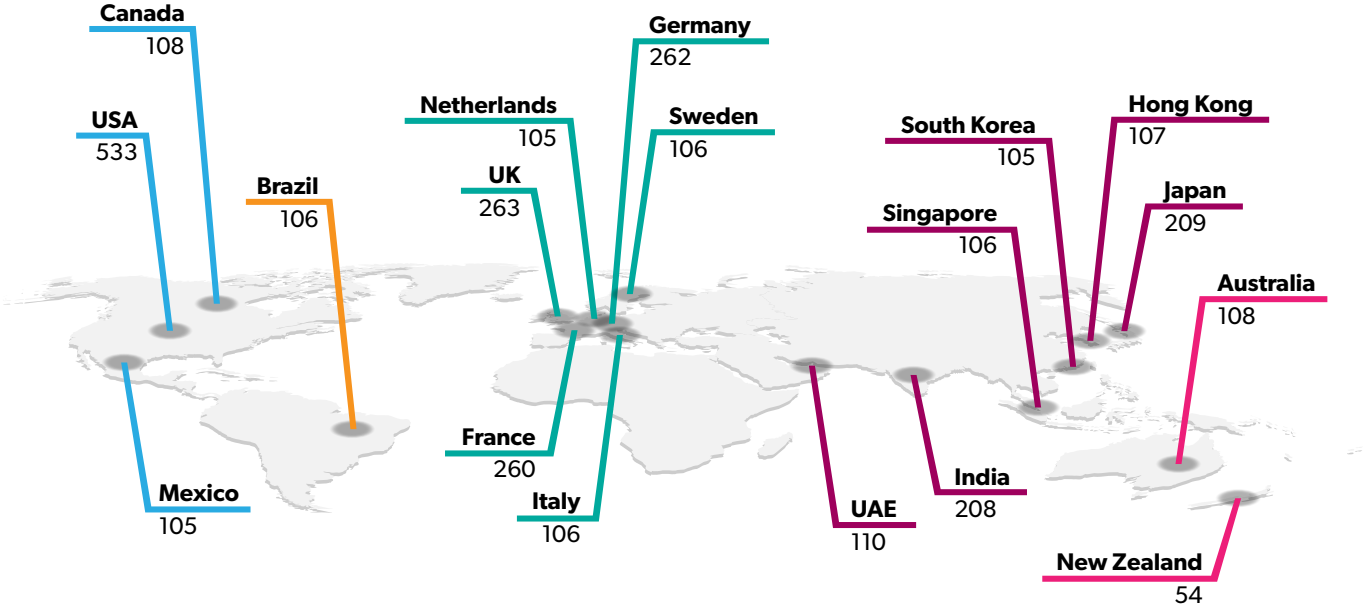
By its nature, critical infrastructure has a broad presence. Whether it be utility services provided to each residence, transportation to each address or communication to each device, CI faces distributed threats, challenges and opportunities. From implementing formal ransomware responses to successful compliance auditing, CI enterprises must take proactive measures that they can control.

New technologies in areas such as 5G, cloud, IAM and GenAI promise new efficiencies when they are programmed into CI operations. Higher expectations and increased commitments around operational resilience and reliability will ultimately drive CI enterprises to a position of greater security and less susceptibility.

About This Study

This research is based on a subset of the global DTR survey of 2,961 respondents that was fielded in November and December 2023 via a web interface and aimed at professionals in security and IT management. This subset data comprises targeted populations in key critical infrastructure industries: energy and utilities, telecommunications, transportation, and trucking/shipping, for a total of 367 respondents across 18 countries.

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. Most respondents (74%) were affiliated with organizations reporting annual revenue between US$100 million and US$999.9 million. This research was conducted as an observational study and makes no causal claims.



Revenue	Number of Respondents
$100m to $249.9m	7
$250m to $499.9m	87
$500m to $749.9m	87
$750m to $999.9m	91
$1 Bn to $1.49 Bn	28
$1.5 Bn to $1.99 Bn	19
$2 Bn or more	48

Industry Sector	Number of Respondents
Energy and Utilities	104
Telecommunications	101
Transportation	87
Trucking / Shipping	75