THALES
Building a future we can all trust

2024 DATA THREAT REPORT

Financial Services Edition

#2024DataThreatReport
cpl.thalesgroup.com

SUPPLEMENT TO GLOBAL EDITION

Financial services (FinServ) organizations, which include banks, investment houses, lenders, finance companies, real estate brokers and insurance companies, are a major component of the world economy. Because they work with a high concentration of sensitive and high-value data, these firms are heavily regulated, and they are prominent targets for cybercriminals. In response, FinServ organizations have some of the highest cybersecurity budgets and advanced defenses. Their top challenges include a rapidly evolving threat landscape, ransomware, insider threats, compliance mandates and third-party risks.

In this executive summary, we share key findings from the 2024 Thales Data Threat Report (DTR) focused on FinServ organizations while examining the differences between FinServ survey respondents and global responses across all industry verticals. Many of the FinServ DTR survey results are similar to overall responses, but we do note some key differences.

Sponsored by

edvance
value added distributor

EXCLUSIVE NETWORKS

netpoleon
Network • Security

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 FinServ organizations that have experienced a breach remains high (39%), but it is 10 percentage points lower than the general survey figure (49%). The percentage of FinServ organizati ons reporting a breach in the last 12 months decreased from 29% in 2021 to 14% in 2024, similar to the survey-wide trend.

39%

About one in five FinServ organizations (18%) report that they have experienced a ransomware attack. This figure is 10 percentage points lower than the overall result and represents a decrease of 17 percentage points from the 2023 DTR Financial Services report. Planning remains poor, with only about one in four FinServ respondents saying they would follow a formal plan in the event of an attack, 5 percentage points higher than among industry group respondents.

18%

Among FinServ organizations, human error was the leading cause of cloud-based data breaches at 41% (10 points higher than overall), and exploitation of previously unknown vulnerabilities was the second highest, 7 percentage points higher than overall. Failure to apply multifactor authentication (MFA) to privileged accounts was another major cause, at 10%, 7 percentage points lower than among all respondents. **FinServ organizations continue to struggle with human error and zero-day vulnerabilities at rates higher than the overall population, while investments in MFA are paying off.**

41%

Identity Complexities and Compromise

On average, **18% of all external access to FinServ organizational IT resources comes from customers,** similar to among overall respondents.

18%

Among survey respondents who cited external identity as an emerging security concern, achieving security consistency across workforce and non-workforce identities is one of the top challenges, cited by 59% of this subset of FinServ respondents.

59%

Increasing DevOps Challenges

61%

Among respondents who cited cloud/DevSecOps security as an emerging security concern, **the greatest proportion, 61% cited secrets management as a top DevOps challenge,** followed by workforce IAM issues such as privileged user management.

Operational complexity remains a security concern, with 49% of FinServ respondents reporting they use five or more key management systems, down 14 percentage points from 2022, and an average of 5.9 key management systems are in use, down 15% from 2022. Interestingly, the percentage of FinServ enterprises saying they have 50 or more SaaS apps in use decreased significantly, from 32% in 2022 to 24% this year. The percentage of organizations using more than one IaaS provider rose from 54% in 2022 to 73% in 2024.

5+

Risks to Emerging Technologies

Regarding threats from quantum computing, future compromise of classical encryption techniques that enable “harvest now, decrypt later” (HNDL) attacks is leading interest in post-quantum cryptography (72% in FinServ, 68% overall). Among FinServ respondents who identified post-quantum cryptography (PQC) as an emerging security threat, 30% indicated they would likely create resilience contingency plans, while 66% said they would prototype or evaluate PQC algorithms in the next 18-24 months. **While FinServ organizations are slightly more concerned about HNDL attacks than the overall population, they are much more involved in evaluating multiple methods to address those concerns.**

72%

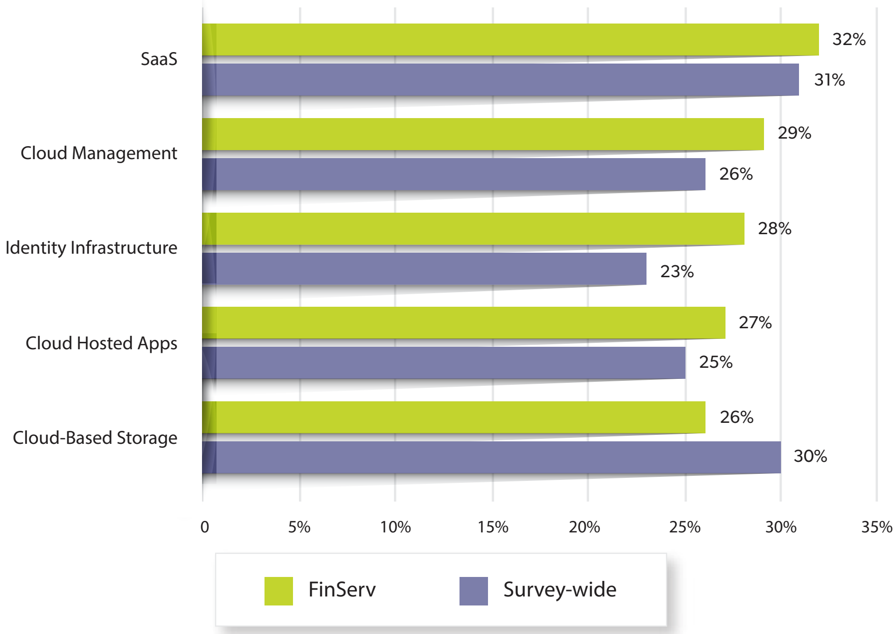
The AI boom is underway: 27% of FinServ respondent organizations plan to integrate AI into their core products and services in the next 12 months, 5 percentage points higher than overall respondents. Only 18% of FinServ organizations are experimenting with AI, compared to 33% of all respondents, likely due to the greater proportion of FinServ respondents already in the pre-integration, enablement phase (44% FinServ versus 27% overall). Managing the associated fast-changing environmental risks is their greatest concern, with 73% of FinServ respondents citing ecosystem and operational alterations as the most concerning risks related to AI and security.

27%

Enterprise Observations

FinServ organizations face greater security challenges in securing cloud infrastructure and focus on locking down secrets in development operations. Among respondents who cited cloud/DevSecOps as a top source of emerging security concern, 61% identified secrets management as a top DevSecOps challenge. Compared to the total survey population, FinServ organizations more commonly cite cloud management infrastructure (consoles, automation tools, secrets, deployment pipelines) as a major target for attackers. It is the second-most-cited target among FinServ organizations, versus fourth survey-wide. The security of cloud infrastructure is critical for FinServ respondents, which chose cloud security as their top spending area.

Top Five Financial Services Attack Targets



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

FinServ respondents are also more likely to note the complexity of securing data in the cloud. Almost two-thirds (64%) of FinServ respondents say it is more complex to secure data in the cloud than on-premises, in contrast with 51% of all enterprises. In addition to these technological challenges, FinServ enterprises must also address their heavy regulatory requirements.

Financial services organizations face heightened cybersecurity regulations across the globe. In the European Union, the Digital Operational Resilience Act will require financial entities to implement contractual, organizational and technical measures to improve the sector's digital resilience by Jan. 17, 2025. In Asia, many financial services organizations need to comply with country-specific regulations such as the technology risk management guidelines of the Monetary Authority of Singapore or India's Digital Personal Data Protection Act. US regulations such as the Bank Secrecy Act and the Gramm-Leach-Bliley Act have been amended over the years to account for cybersecurity. Compliance with security policies to address multiple regulations and regulators will remain a challenge for financial service organizations.

While financial organizations worldwide face a heavy regulatory landscape, compliance achievement correlates with better security outcomes. In the 2024 survey, among FinServ respondents whose organizations failed a compliance audit in the last 12 months, 80% reported at least one breach in their history, similar to respondents across all industries. In contrast, for those FinServ organizations that passed all compliance audits, only 15% have a breach history, and just 3% had a breach in the last 12 months.

KEY STATISTIC

In 2024, among FinServ respondents whose organizations failed a compliance audit in the last 12 months, 80% reported at least one breach in their history.

80%

KEY STATISTIC

In contrast, for those FinServ organizations that passed all compliance audits, only 15% have a breach history, and just 3% had a breach in the last 12 months

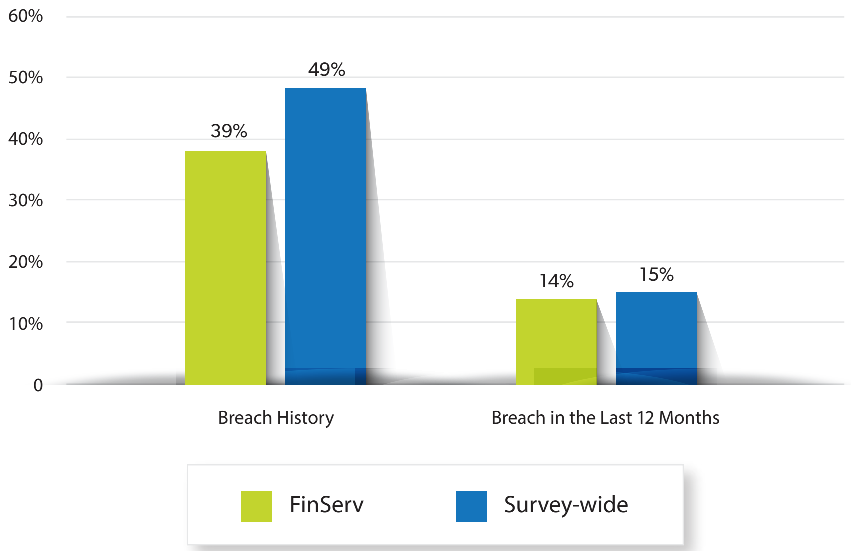
15%

The Threat Landscape

In FinServ organizations, as in the rest of the world, the attack landscape remains vast and growing. **Almost all FinServ respondents (95%) said they saw an increase in attacks, nearly double the percentage in 2022 (50%).** The top three fastest-growing types of threats reported by FinServ organizations were malware, application vulnerabilities and phishing. Compared with the 2022 DTR FinServ survey, malware retained first place, while application vulnerabilities replaced ransomware for second place and phishing replaced credential stuffing for third place. This makes sense as many attacks today begin with a phishing attack, followed by exploitation of an application vulnerability and then deployment of malware that enables remote command and control and lateral movement within the organization.

Internal human error was the top cause of cloud-based data breaches and the most common threat actor. Correlating threat actors with the causes of cloud-based data breaches shows that for all threat actors, including hacktivists, external cybercriminals and even malicious insiders, the top vector enabling exploitation is human error. **Within FinServ organizations, top exploitations and root causes of cloud data breaches were human error (41%), unknown vulnerabilities (31%) and known vulnerabilities (18%).** In the case of malicious insiders with non-financial motivations, exploiting unknown/novel/zero-day vulnerabilities tied as the top cause. Human error can be mitigated with usable security such as strong MFA, context-aware audit logs and understandable classification schemes.

Overall Breach History and Recent Breach History



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

The Attack Surface

Within FinServ organizations, reducing attack surfaces involves understanding technological and organizational dynamics. **Ransomware response remains a challenge:** Over the last three years, fewer than 50% of respondents across all verticals reported having a formal ransomware plan in place — and only 25% of FinServ respondents have one, despite regulations increasingly requiring them. Among FinServ respondents that have resolved a past ransomware attack, 5% did so by paying a ransom, while 9% said they would pay a ransom to resolve a future attack. Ransomware and breach responses draw greater scrutiny as they are increasingly led by legal teams interfacing with regulators or law enforcement.

Technologically, the complexity of cloud resources among end users, operators and developers continues to grow. While the average number of SaaS applications in use by financial services organizations is identical to the overall average (84), the percentage of FinServ organizations using more than one hyperscale cloud provider (IaaS) rose from 54% in 2022 to 73% in 2024 — an increase of 19 percentage points. The percentage of FinServ respondents who agree or strongly agree that managing security in the cloud is more complex than on-premises has risen 20 percentage points since 2022 — 15 percentage points more than the increase in the overall survey result — indicating that these organizations feel the pain of increasing cloud complexity more acutely than their counterparts in other industries.

FinServ respondents also report that, on average, 44% of their data stored in the cloud is sensitive, reaffirming that these organizations are moving critical workloads to the cloud. Meanwhile, 23% of FinServ respondents depend on cloud providers to control the encryption keys for more than half of applications, similar to the overall survey population (26%). For those keys specifically under their control, 35% of FinServ respondents have chosen the "bring your own key" (BYOK) approach, a figure that has doubled since 2022.

Attack surfaces within and among FinServ organizations will continue to grow due to new technology adoption. The speed of AI adoption and the technology's fast-moving ecosystem has emerged as a significant security concern. Nearly three-fourths (73%) of FinServ respondents cite rapid changes as a challenge impacting their existing AI plans, yet 71% also report that they are in the integration or enablement phases of production deployments, beyond experimentation or exploration phases.

KEY STATISTIC

FinServ respondents report on average, 44% of their data stored in the cloud is sensitive, reaffirming that these organizations are moving critical workloads to the cloud.

44%

Emerging Concerns

This year's DTR survey asked respondents to select their top four areas of security concern among emerging technologies, including cloud and DevSecOps, AI, workforce identity and access management (IAM), IoT/5G, PQC and digital sovereignty. FinServ organizations most frequently cite concerns with cloud security and DevSecOps, followed by external identity, digital sovereignty, IoT and then AI.

When asked what aspects of 5G security are the most concerning, two-thirds (67%) of FinServ respondents cited the data moving over 5G networks as their top worry, followed by protecting the identities of devices, people and things connected to 5G networks (62%). Thirty-two percent of FinServ organizations identified IoT devices as one of their greatest 5G-related security concerns.

KEY STATISTIC

Nearly three-quarters (72%) of FinServ respondents report that future encryption compromise is the top concern among security threats related to quantum computing.

72%

Nearly three-quarters (72%) of FinServ respondents report that future encryption compromise is the top concern among security threats related to quantum computing, similar to the overall survey result. Thirty percent of FinServ respondents say they will create resilience contingency plans to satisfy quantum computing security concerns in the next 18-24 months, 14 percentage points below the survey-wide result.

Access Control

There is a bit of a sea change underway in terms of how access control is managed, and by whom. **Nearly half (43%) of FinServ respondents in the latest survey agree that organizations should maintain control over their access security, compared with 26% in the 2022 survey, indicating that organizations are increasingly using internal staff for access security.** Moreover, 32% of FinServ 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 (30%) — while 48% agree that an agnostic access management solution can best protect multicloud environments.

Among FinServ respondents, 73% say that MFA is a technology they have chosen to secure access to data in the cloud (on par with the overall result 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.

KEY STATISTIC

About two in five FinServ respondents (41%) agree that access management and authentication plays a key role in achieving zero-trust security. Having more than 50 SaaS apps necessitates a deeper dive into authentication journeys.

41%

About two in five FinServ respondents (41%) agree that access management and authentication plays a key role in achieving zero-trust security. Having more than 50 SaaS apps necessitates a deeper dive into authentication journeys. Enabling zero-trust with the plethora of SaaS apps and disparate users requires flexible access policies. Similarly, for legacy environments, an on-premises authentication solution remains necessary to protect resources.

Next Steps

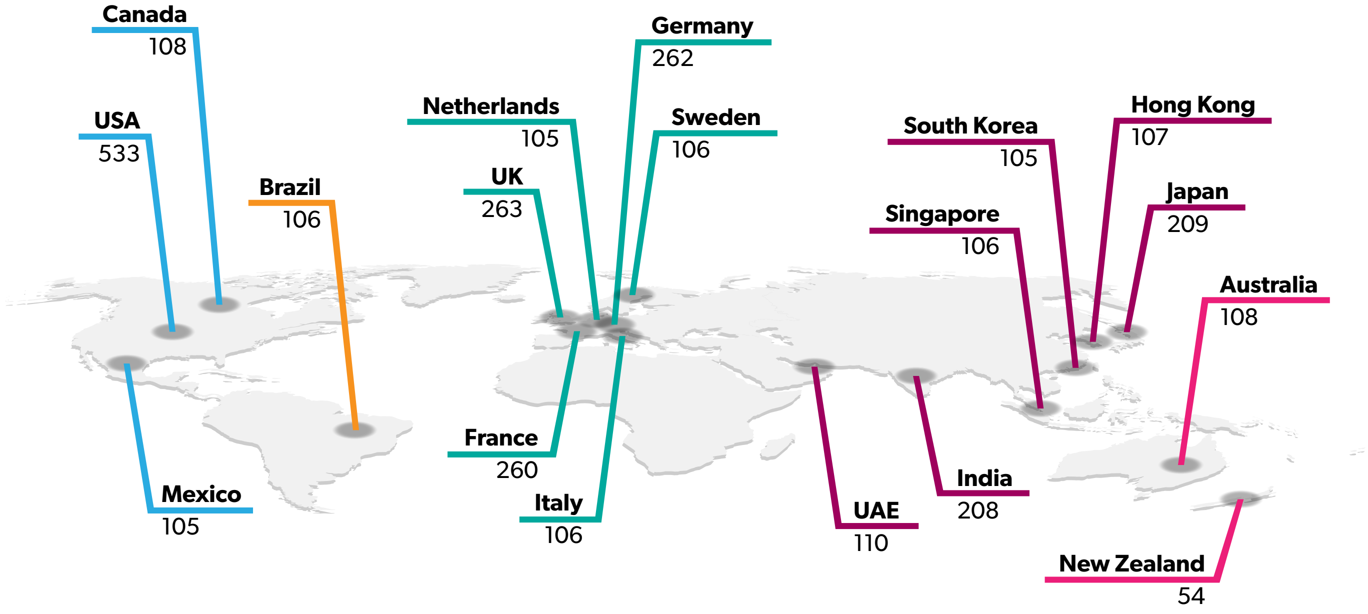
By their nature, financial services organizations have disparate and highly distributed architectures supporting users that range from executives and headquarters staff to retail branches and customers. Whether they provide banking services, insurance, investment banking or securities, these organizations face highly sophisticated threats, challenges and opportunities. From implementing formal ransomware responses to successful compliance auditing, financial services 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 FinServ operations. Higher expectations and increased commitments to operational resilience and reliability will ultimately drive these enterprises to a position of greater security and less susceptibility.

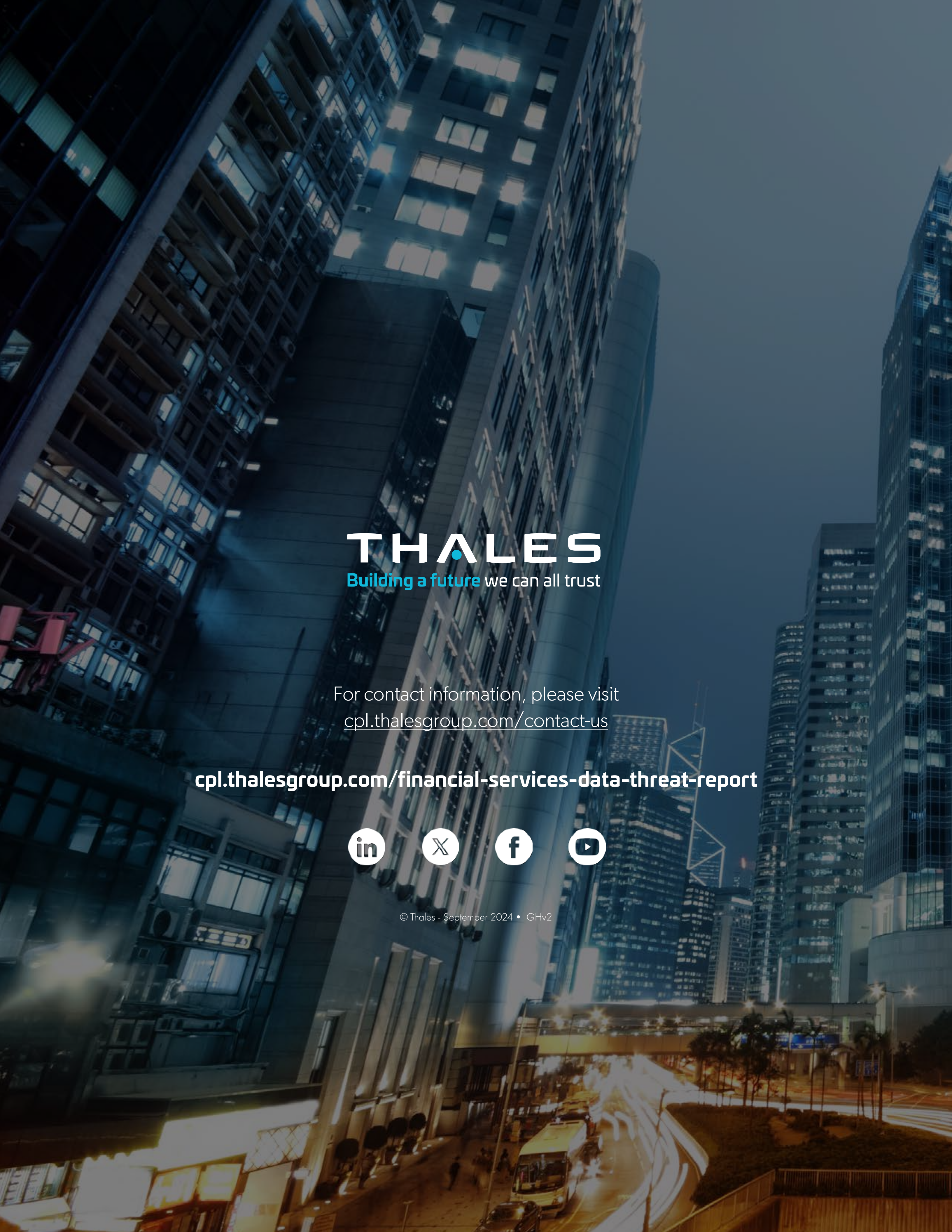
About This Study

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 a targeted financial services population, for a total of 108 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 (70%) 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	2
$250m to $499.9m	16
$500m to $749.9m	26
$750m to $999.9m	32
$1 Bn to $1.49 Bn	12
$1.5 Bn to $1.99 Bn	4
$2 Bn or more	16



THALES

Building a future we can all trust

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

cpl.thalesgroup.com/financial-services-data-threat-report