Understanding Data Security Risk

Survey Report

Release Date: 02/2025

cloud security alliance®

Overview

1. Methodology and Goals for the Survey
2. Key Findings
3. Demographics
4. About the Sponsor

Survey Creation and Methodology

Survey Creation

- Approached by sponsor/member
- Outline overarching questions
- Develop large question pool
- Refine final questionnaire

Data Collection

- Distribute online survey in October 2024
- Received 912 responses

Analysis and Report

- Research team analyzes data
- Identify 4-7 most interesting or surprising findings
- Write report based on team's analysis

Goals of the Study:

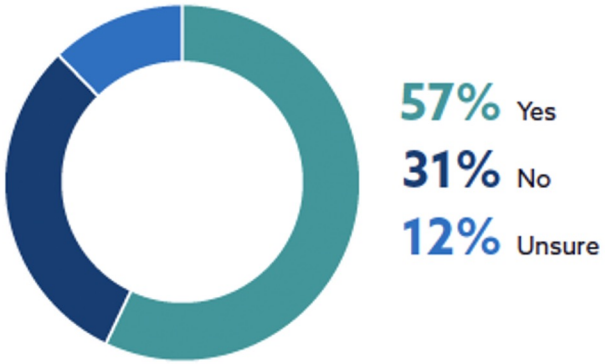
This survey aims to understand how organizations assess and manage cybersecurity and data risks. It focuses on:

- **Methods for Assessing Data Risk**: How organizations evaluate risks across data assets in on-premises, hybrid, and cloud environments.
- **Tools and Automation for Risk Evaluation**: The tools used to monitor and mitigate risks, with a focus on automation to improve efficiency.
- **Challenges and Priorities**: Key obstacles in risk evaluation, such as resource limitations and siloed tools, and priorities for improvement

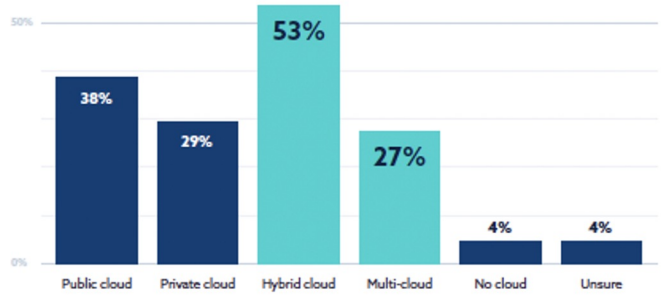
Key Finding 1:Gaps in Understanding Risk

- **Risk Identification Challenges**:
  - 31% lack tools to identify riskiest data sources.12% unsure if such tools are available.
  - 80% lack confidence in identifying high-risk data sources.
  - Limited ability to act on insights from existing tools due to low maturity in risk management practices.
- **Complex Environments Increase Risk**:
  - Large organizations face more fragmented risk profiles due to diverse systems.
  - Inconsistent management practices increase likelihood of undetected risks.
- **Recommendations**:
  - Invest in solutions that provide actionable insights into data risks and their impact.
  - Strengthen risk management strategies to safeguard sensitive assets in complex environments.

Tools to identify number of data sources that are riskiest



Cloud computing models used



Most helpful features for understanding organizations' data risk

36% Assessment results
34% Dedicated dashboard
34% Risk score

31% Near-real-time alerts
30% Real-time reports
23% Threat levels
21% Behavioral analytics

19% Audit logs
15% Industry trends
15% Contextualizing multiple data feeds
12% Recommendations for decreasing risk score

Key Finding 2: Misalignment Between Management and Staff Impacts Risk and Compliance Strategies

Strategic vs. Operational Priorities:

- Executives focus on high-level goals (e.g., quantifying security posture, aligning with business priorities).
- Staff prioritize securing resources to implement strategies.

Disconnect in Perceptions:

- 20% of staff feel CISOs don't prioritize executive investment in security, vs. 34% of management who do.
- Staff less confident in identifying high-risk data sources (10% vs. 3% of management).

Operational Challenges:

- 48% cite limited staffing; 46% lack automation.
- 54% rely on semi-automated processes; 22% use manual methods.

Recommendation:

- Improve communication and collaboration between management and staff.
- Prioritize investments in resources, automation, and process improvements to bridge execution gaps.

Key Finding 3: Existing Tools Struggle to Keep Pace with Evolving Modern Risk Management Needs

Tool Overload and Inefficiencies:

- 54% use four or more tools, leading to inefficiencies and conflicting information.
- 26% report siloed tooling as a barrier to effective risk management.

Tool Limitations:

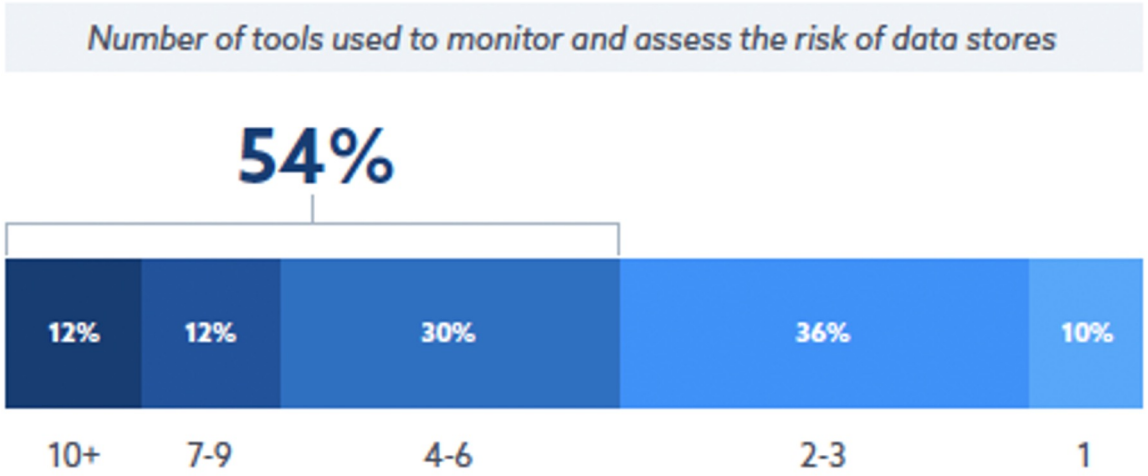
- Traditional tools lack integration and visibility for proactive data risk management.
- Disconnected tools hinder the ability to identify and manage interconnected risks.

Complex Environments Amplify Challenges:

- Hybrid and multi-cloud setups require tools that scale, integrate, and provide real-time insights.

Recommendation:

- Adopt unified platforms that integrate compliance, security, and risk management.
- Streamline processes and improve visibility for proactive risk identification and response.



Key Finding 4: Regulations and Compliance Drive Risk Reduction but Fall Short on Proactive Data Security Strategies

Compliance Drives Risk Strategies:

- 59% prioritize compliance (e.g., ISO, GDPR, PCI DSS) for risk reduction.
- Compliance ensures operational continuity and avoids penalties.

Reactive Approach to Emerging Risks:

- Only 11% prioritize risky user behavior; 12% focus on adapting to changing attack surfaces.
- 15% perform real-time risk evaluations; 31% take over a week to assess risks.

Gaps in Addressing Dynamic Threats:

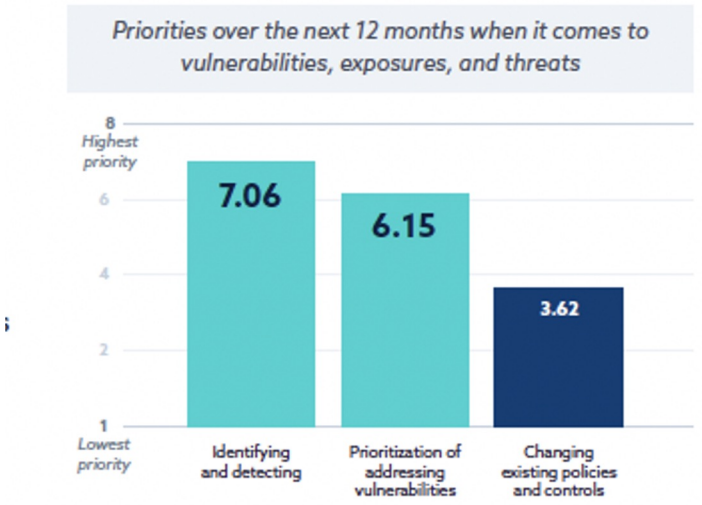
- Compliance alone fails to address evolving threats and expanding attack surfaces.
- Delays in risk evaluation leave vulnerabilities unaddressed.

Recommendation:

- Balance compliance with proactive strategies like real-time monitoring, advanced detection, and dynamic risk evaluation.

Key Finding 5: A Shift Toward Risk-Based Strategies Is Critical

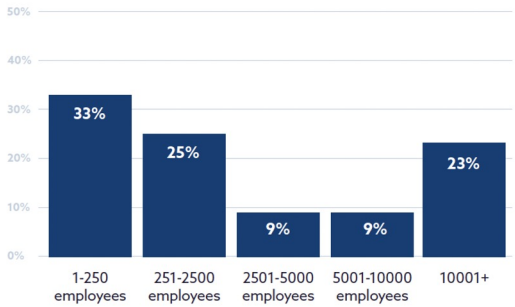
- **Organizations are shifting from compliance-driven to risk-based security strategies.**
  - **Top Priorities:** Identifying (7.06) and prioritizing (6.15) vulnerabilities—far exceeding policy changes (3.62).
- **Key Performance Indicators:**
  - **Vulnerability patch rate (36%)** and **security violations (35%)** prioritized over **compliance violations (29%)**.
- **Investment Focus (Next 12–18 Months):**
  - **Training staff (65%)**, streamlining processes (51%), consolidating tools (47%).
- **Why It Matters:**
  - Risk-based strategies improve **resilience, efficiency, and proactive risk reduction** while streamlining compliance as a secondary benefit.
- **Call to Action:** Accelerate the transition to risk-based security for **better risk management, security outcomes, and operational efficiency**.



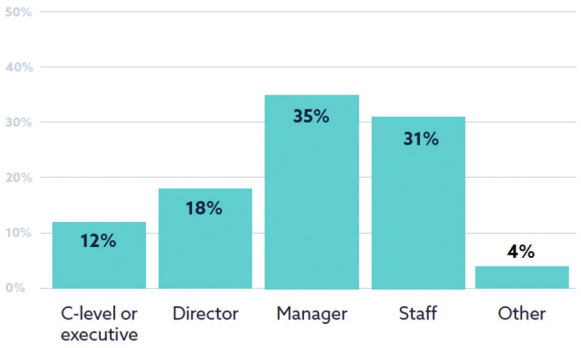
Demographics

Total of 912 responses

Organization size

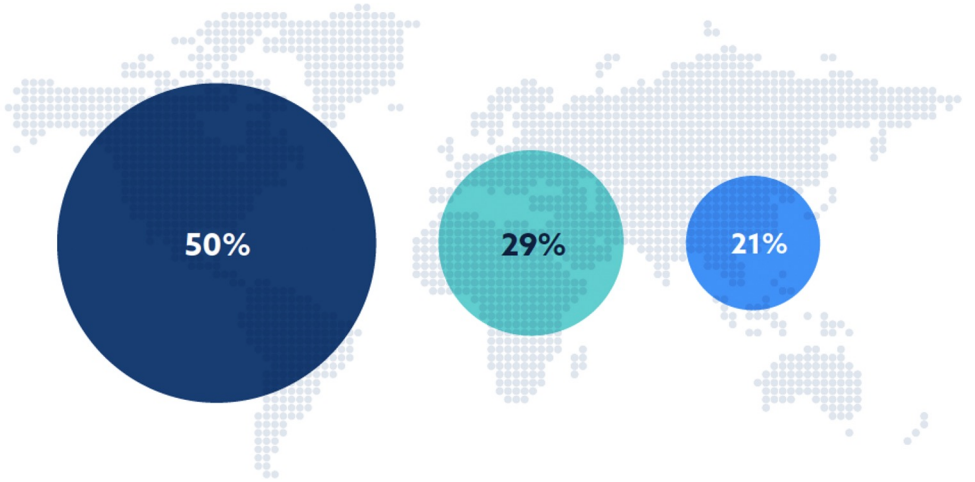


Which best describes your job level?



What region of the world are you located in?

- Americas
- Europe, Middle East, Africa (EMEA)
- Asia Pacific (APAC)



Which of the following best describes the principal industry of your organization?

31%	Telecommunications, Technology, Internet & Electronics	2%	Transportation & Delivery	1%	Automotive
18%	Finance & Financial Services	2%	Business Support & Logistics	1%	Nonprofit
7%	Government	2%	Utilities, Energy, and Extraction	1%	Real Estate
7%	Education	2%	Airlines & Aerospace (including Defense)	1%	Construction, Machinery, and Homes
6%	Prefer not to answer	2%	Entertainment & Leisure	1%	Health & Fitness
6%	Healthcare & Pharmaceuticals	1%	Insurance	1%	Food & Beverages
3%	Manufacturing	1%	Advertising & Marketing	1%	Agriculture
2%	Retail & Consumer Durables	1%	I am currently not employed		

About the Sponsor

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. As the global leader in security for a world powered by Applications, Data, Identities, and Software, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day. Thales Cloud Protection & Licensing is part of Thales Group. For further information, visit cpl.thalesgroup.com.

THALES

Building a future we can all trust