


Understanding Data Security Risk

2025 Survey Report





© 2025 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at <https://cloudsecurityalliance.org> subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

云安全联盟

创立于2009年,作为世界领先的独立、权威国际产业组织,致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识和全面发展。

云安全联盟大中华区

在香港注册并在上海登记备案的国际NGO组织,旨在立足中国,连接全球,推动中国数字安全技术标准与产业的发展及国际合作。



4 大区

大中华区、美洲区、
欧非区、亚太区



180+ 分会

英国、法国、加拿大、旧金山、马来西亚等覆盖50多个国家和地区



2.5K+ 成员单位

世界500强科技公司、安全厂商、中小型企业、研究机构



20w+ 社区专业人员

研究工作组专家、社区志愿者、从业人员、CSA认证学员



前沿研究

#云安全 #AI安全
#零信任 #数据安全
#5G安全 #区块链安全
#量子安全 #物联网安全
#金融安全 #医疗安全
#智能座舱安全
#关键基础设施安全
.....



培训与认证

CCSK 云安全知识认证
CDSP 数据安全认证专家
CAISP人工智能认证专家
CZTP 零信任认证专家
CCPTP 云渗透测试认证专家
CCAK 云计算审计知识认证
.....



会议活动

CSA summit@RSAC
CSA GCR Congress
CSA研讨会
AI For GOOD峰会
.....



评估与认证

AI STR AI安全、可信、负责任认证
STAR 云安全评估认证
CAST 云应用安全可信认证
CNST 云原生安全可信认证
.....

1000+研究成果

10W+认证学员

1000W+传播量

成员单位(部分)



企业合作微信号:csagcr



认证培训微信号:CSAlynn



邮箱:info@c-csa.cn



Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Marina Bregkou
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

Special Thanks

Lynne Murray, Krishna Ksheerabdhhi, and Brian Robertson

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 Cybersecurity Products is part of Thales Group. For further information, visit cpl.thalesgroup.com.



Table of Contents

Acknowledgments.....	3
Lead Author.....	3
Contributors	3
Graphic Design	3
Special Thanks.....	3
About the Sponsor	3
Executive Summary	5
Key Findings	6
Gaps in Risk Understanding Limit Effective Risk Management.....	6
Misalignment Between Management and Staff Impacts Risk and Compliance Strategies.....	8
Existing Tools Struggle to Keep Pace with Evolving Modern Risk Management Needs	10
Regulations and Compliance Drive Risk Reduction but Fall Short on Proactive Data Security Strategies	11
A Shift Toward Risk-Based Strategies Is Critical	12
Final Thoughts on the State of Data Security Risk	14
Full Survey Results.....	15
Overview	15
Concerns and Challenges	16
Risk Evaluation Strategy	17
Risk Management Tools.....	20
Compliance and Standards	21
Program Strategy and Drivers.....	21
Demographics	23
Survey Methodology and Creation	24
Goals of the Study	24

Executive Summary

Organizations today face a rapidly changing threat landscape, where the complexities of hybrid and multi-cloud environments expose new vulnerabilities and challenge traditional information security and risk management strategies. This survey reveals critical insights into the obstacles organizations encounter, including a fragmented stack of security, privacy, and data management tools, confidence gaps in risk understanding, and misaligned priorities between leadership and operational teams. While these challenges are significant, the findings also highlight actionable opportunities for organizations to rethink their strategies and embrace proactive approaches to secure their most sensitive assets.

Key findings from the survey include:



1. Gaps in Understanding Risk

Many organizations lack the tools and confidence to identify high-risk data sources, with 31% reporting insufficient tooling and only 20% expressing high confidence in their ability to address these risks. This reflects a broader need for actionable insights to prioritize and mitigate vulnerabilities effectively.



2. Misaligned Priorities

Diverging focuses between management and staff create inefficiencies. Executives (43%) prioritize aligning data security efforts with broader business objectives, while operational teams face resource constraints and rely heavily on manual or semi-automated processes. Bridging this gap is essential for cohesive risk and compliance strategies.



3. Inefficient Tools

Over half of organizations use four or more tools to manage data risks, leading to inefficiencies and conflicting information. Traditional compliance and security tools, while essential, often lack the scalability and integration needed for modern data risk management.



4. Compliance vs Threat-based Strategies

Compliance remains a primary driver for risk reduction (59%), but a heavy focus on regulatory adherence often leaves organizations unprepared for emerging threats. Real-time monitoring, dynamic risk evaluation, and proactive measures are critical to addressing these gaps.



5. Shift to Risk-Based Strategies

Organizations are beginning to prioritize risk-based approaches, with identifying and prioritizing vulnerabilities ranking as top priorities. Forward-looking investments in training, process streamlining, and tool consolidation further signal this shift.

Organizations must evolve their strategies to effectively navigate today's complex risk landscape. By enhancing risk understanding, aligning priorities across teams, integrating siloed tools into unified platforms, and embracing proactive, risk-based approaches, organizations can improve resilience, safeguard critical data assets, and achieve compliance more efficiently. These steps provide a clear pathway toward a stronger, more adaptive security posture.

Key Findings

In an era of complex hybrid and multi-cloud environments, organizations are grappling with the nuance of identifying, prioritizing, and mitigating risks that threaten their most sensitive assets. The results of this survey reveal not just the challenges—gaps in risk understanding, misaligned priorities, and tool inefficiencies—but also the opportunities for organizations to strengthen their security posture. By embracing a deeper understanding of data risks, organizations can close confidence gaps, streamline operations, and stay ahead of evolving threats.



Key Finding 1:

Gaps in Risk Understanding Limit Effective Risk Management

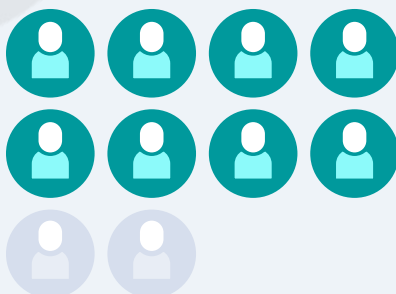
Organizations face significant challenges in managing data risks due to gaps in their ability to effectively identify and prioritize vulnerabilities. For instance, **31% of respondents lack tools to identify their riskiest data sources**, and an **additional 12% are unsure** if they have such tools. This lack of adequate tooling creates blind spots that hinder proactive risk management, leaving critical vulnerabilities unaddressed.

Tools to identify number of data sources that are riskiest



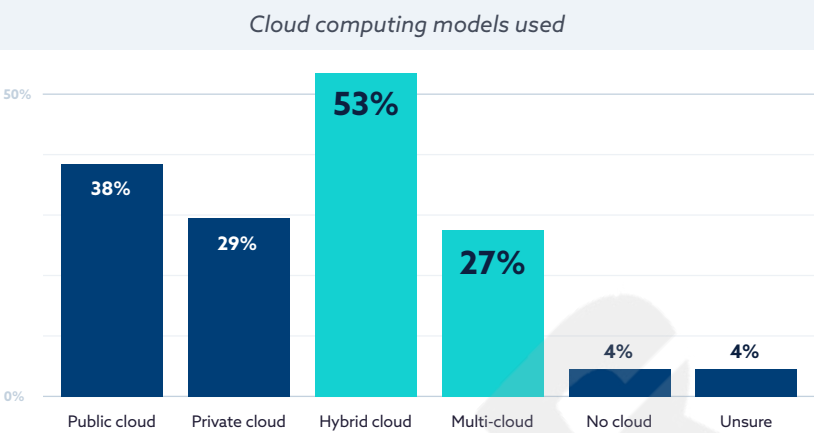
57% Yes
31% No
12% Unsure

80% of respondents do not feel highly confident in their ability to identify high-risk data sources



Coupled with this, **80% of respondents** do not feel highly confident in their ability to identify high-risk data sources. This low confidence highlights a broader challenge: even when tools are in place, organizations struggle to interpret or act on the insights these tools provide, reflecting a lack of maturity in risk management practices.

The complexity of hybrid and multi-cloud environments further compounds these issues. Over half of respondents **(53%) operate in hybrid environments**, and **27% use multi-cloud setups**, with large organizations (>10,000 employees) adopting these strategies more frequently. These environments, while offering flexibility and scalability, also create fragmented risk profiles, making it more difficult to locate and prioritize vulnerabilities. As data is distributed across diverse systems, inconsistencies in management practices exacerbate these challenges, increasing the likelihood of undetected risks.



Despite these gaps, organizations are beginning to recognize the value of tools that provide actionable insights into data risks by leveraging multiple risk indicators. Features like **assessment results (36%)**, **dedicated dashboard (34%)**, and **risk scores (34%)** are prioritized by organizations to help make sense of their data landscapes and direct remediation efforts effectively. This focus reflects a growing understanding that actionable insights—not just visibility—are essential for addressing risks in complex environments. These features are also viewed as critical tools for guiding risk-focused remediation efforts and enabling a more proactive response to emerging threats.



Effectively managing data risks requires organizations to close gaps in understanding by investing in solutions and processes that provide actionable insights (e.g., visibility, risk assessment, risk posture insights) into where risks exist, their causes, and their potential impact. Addressing these gaps holistically will not only build confidence in risk management strategies but also strengthen organizations' ability to proactively safeguard their sensitive assets across distributed data infrastructures and hybrid cloud environments.



Key Finding 2:

Misalignment Between Management and Staff Impacts Risk and Compliance Strategies

A significant gap exists between the strategic priorities of management and the operational realities faced by staff, which undermines the effectiveness of risk and compliance strategies. Executives' focus on strategic goals in the next 12 months, such as identifying and addressing vulnerabilities and maintaining strong communication about security posture, underscores the importance of aligning these priorities with operational realities. However, executives report Chief Information Security Officers (CISOs) prioritize high-level objectives, such as **"Quantifying the organization's data security posture" (46%)**, **"Balancing security initiatives with operational efficiency" (41%)**, and **"Aligning security efforts with broader business priorities" (40%)**, while staff focus more on securing resources to implement these strategies.

Executive's perceptions of CISO's focus when communicating data security



46%

Quantifying the organization's data security posture



41%

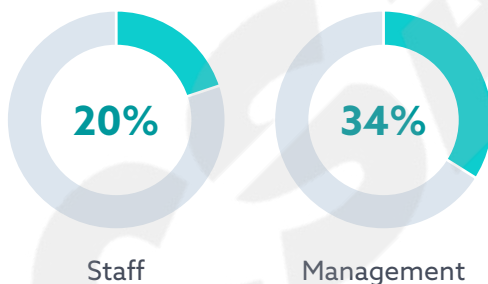
Balancing security initiatives with operational efficiency



40%

Aligning security efforts with broader business priorities

Perceptions of CISO's prioritization of convincing executives to invest in security measures



"not at all confident" (10%) in identifying high-risk data sources, compared to **3% of management**. This lack of confidence among those executing risk management processes indicates operational barriers that are not fully addressed by management's strategic plans.

For instance, only **20% of staff** believe CISOs prioritize convincing executives to invest in security measures, compared to **34% of management** who view this as a priority. This divergence highlights a disconnect in how data security risk management needs are perceived and addressed at different organizational levels.

This misalignment is further reflected in confidence levels regarding risk understanding. Staff are significantly more likely to report being

Confidence in organizations ability to identify high-risk data sources

C-Level



Staff



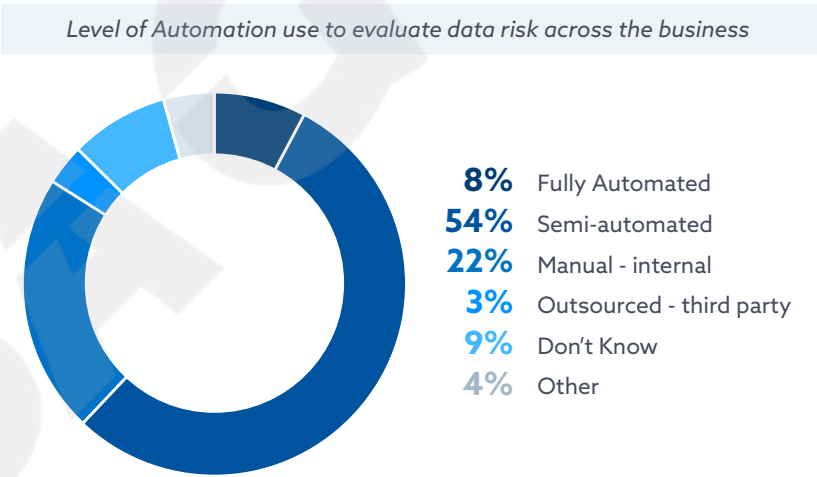
■ Highly confident ■ Moderately confident ■ Somewhat confident ■ Not at all confident

Operational challenges further compound these issues. **48% of respondents cite limited staffing**, and **46% point to a lack of automation** as key barriers.



These constraints force many teams to rely on inefficient methods: **54% rely on semi-automated processes**, while **22% still depend entirely on manual processes** for risk evaluation. These gaps in resources and automation conflict with management's focus on aligning security efforts with broader business objectives, resulting in delays, inefficiencies, and missed vulnerabilities.

The misalignment between management's strategic goals and staff's operational needs creates execution gaps that weaken security, risk, and compliance strategies. To bridge this divide, organizations must improve communication and collaboration between these groups, ensuring that strategic plans are informed by operational realities. This includes prioritizing security investments in resources, automation, and process improvements to enable staff to meet management's goals effectively. Aligning priorities at all levels will create a more cohesive approach to managing risks and achieving compliance.

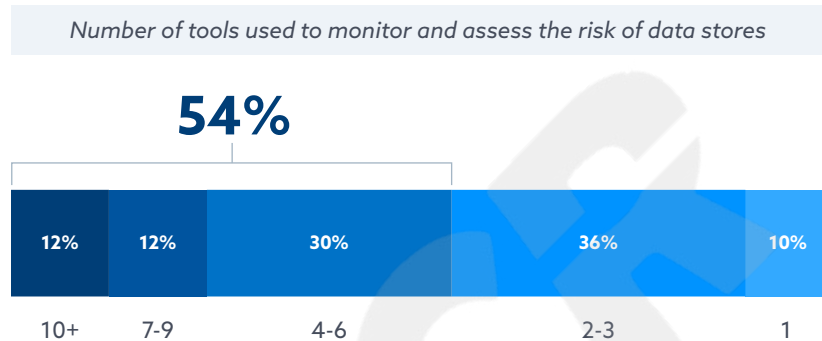




Key Finding 3:

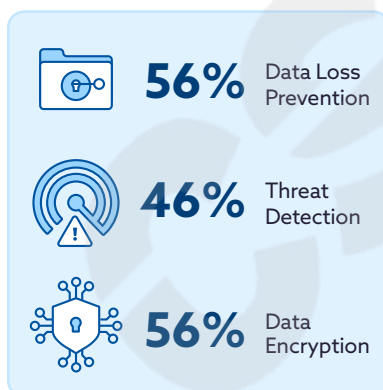
Existing Tools Struggle to Keep Pace with Evolving Modern Risk Management Needs

Organizations are increasingly dependent on a variety of tools to manage compliance, security, and risk, yet many of these tools fail to meet the demands of modern data risk management. **Over half of organizations (54%) use four or more tools** to manage data risks, potentially creating inefficiencies and conflicting information that could hinder effective decision-making. This proliferation of tools not only complicates workflows but also increases the likelihood of siloed processes: **26% of respondents cite siloed tooling as a barrier** to effective risk management.



While compliance tools are widely adopted, they often lack the features necessary for proactive data security and risk posture management. Traditional tools, such as **Data Loss Prevention (56%)**, **Threat Detection (46%)**, and **Encryption (56%)** are critical for security and compliance but fall short in providing visibility and integration capabilities essential for modern digital landscapes. Furthermore, the use of many disparate and often siloed tools can make it challenging for organizations to identify interconnected risks or holistically manage them across different teams and departments. These gaps suggest that organizations are not fully leveraging technologies that can contextualize, prioritize, and provide actionable insights into data security threats and risk mitigation.

Tools used to manage data risk



These challenges are amplified in dynamic and complex environments. Hybrid and multi-cloud architectures demand tools that can scale, integrate seamlessly, and provide real-time insights into risk. The reliance on compliance-focused tools leaves organizations unable to adapt to evolving threats, which require dynamic and integrated risk management approaches.

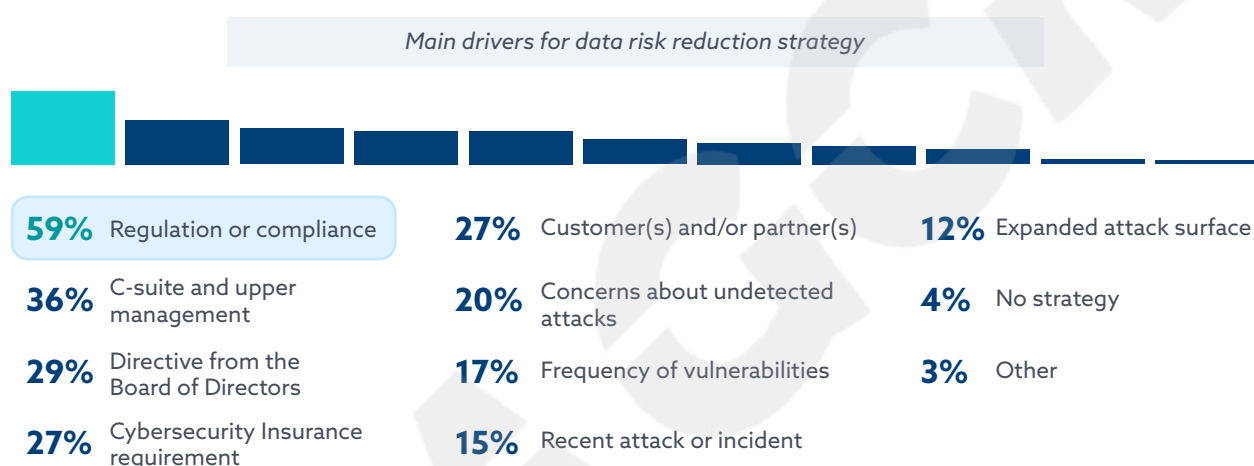
Organizations face significant challenges in managing modern data risks, largely due to their reliance on disjointed and compartmentalized security tools. This fragmented approach creates inefficiencies, hinders visibility, and limits the ability to respond to emerging threats effectively. Adopting more unified platforms that bring together compliance, security, and risk management capabilities can help streamline processes and improve visibility. By taking a more integrated approach, organizations can gain the insights needed to identify and address risks proactively, ultimately enhancing their resilience and adaptability in an evolving threat landscape.

Key Finding 4:



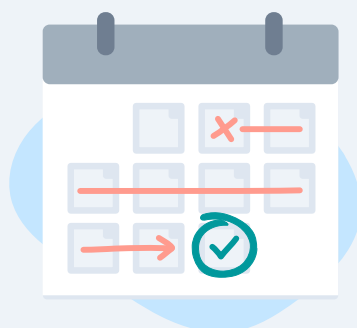
Regulations and Compliance Drive Risk Reduction but Fall Short on Proactive Data Security Strategies

Regulations and compliance remain the dominant forces shaping organizations' risk management strategies. **59% of respondents prioritize regulation and compliance** as the primary drivers for risk reduction, with **ISO (51%)** and **GDPR (50%)** being the most commonly adhered-to frameworks, followed by **PCI DSS (45%)**. These frameworks help organizations maintain operational continuity and avoid penalties, making compliance an essential part of their security posture.



However, a strong focus on compliance often leaves gaps in addressing emerging and evolving risks. For instance, only **11% of respondents prioritize identifying risky user behavior**, and just **12% focus on adapting to the changing attack surface**. These figures indicate that many organizations are reactive, concentrating on compliances rather than proactively protecting data and mitigating risky behaviors in order to assure critical business functions continue without major setbacks due to data breaches or security incidents. This further suggests that organizations are not adequately addressing emerging risks and adequately adapting to changing attack surfaces.

Only **15%** of respondents perform real-time risk evaluations, while **31%** take more than one week to assess risks across business units and assets



This reactive approach is further highlighted by sporadic risk evaluation of critical assets including databases, data repositories, file servers, cloud platforms, and storage systems. Only **15% of respondents perform real-time risk evaluations**, while **31% take more than one week to assess risks**

across business units and assets. These delays in evaluation leave vulnerabilities unaddressed for extended periods, increasing the likelihood of exposure to new and emerging threats.

Regulatory compliance alone is not enough to safeguard sensitive data. As attack surfaces expand and threat landscapes evolve, organizations must move beyond compliance-focused strategies to adopt proactive measures that address risks dynamically and holistically.

While compliance frameworks provide critical structure, security controls, measures, as well as ensure adherence to industry standards, they fall short of equipping organizations to tackle emerging risks and evolving attack surfaces. To bridge this gap, organizations must balance compliance requirements with proactive risk management strategies that include real-time monitoring, advanced threat detection, and dynamic risk evaluation. By investing in tools and processes that go beyond regulatory mandates, organizations can build a more resilient and forward-looking security posture while ensuring the stability of critical business operations even during cyberattacks or security incidents.

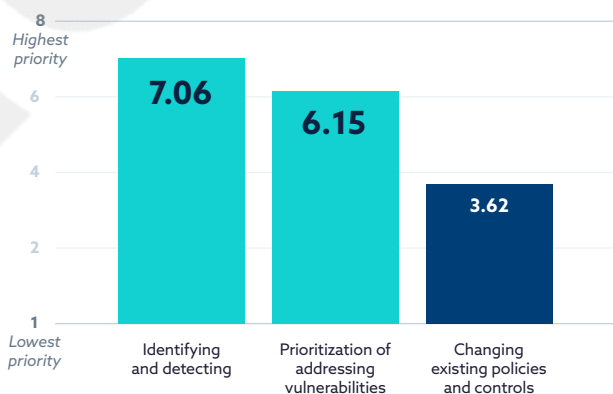


Key Finding 5:

A Shift Toward Risk-Based Strategies Is Critical

As the complexity of modern data environments grows, organizations are beginning to recognize the limitations of compliance-driven strategies and are shifting toward risk-based approaches. **Identifying vulnerabilities (7.06)** and **prioritizing vulnerabilities (6.15)** are ranked as the highest priorities by respondents, far outpacing activities such as changing policies and controls (3.62). This focus signals a clear emphasis on proactive risk reduction over reactive compliance measures.

Priorities over the next 12 months when it comes to vulnerabilities, exposures, and threats



Key risk indicators organizations use



36%

Vulnerability patch rate



35%

Security violations

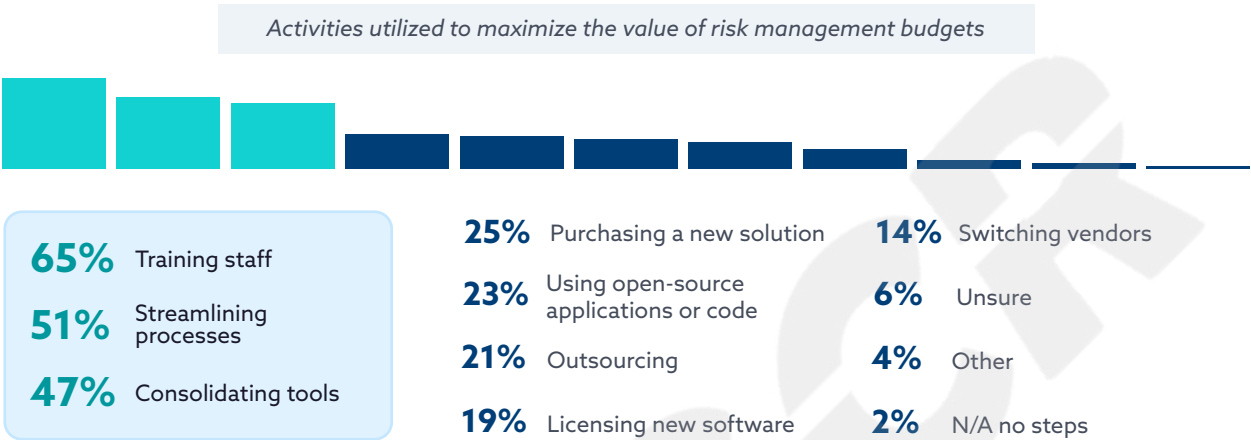


29%

Compliance violations

Metrics further support this trend, with **vulnerability patch rate (36%)** and **security violations (35%)** prioritized over **compliance violations (29%)** as key performance indicators. These metrics highlight a growing recognition that reducing vulnerabilities and managing risks directly contributes to organizational resilience, going beyond the requirements of regulatory frameworks.

Additionally, the types of features organizations value for understanding risks reflect a shift toward actionable insights. This is complemented by forward-looking investment plans: over the next 12-18 months, organizations are prioritizing **training staff (65%)**, **streamlining processes (51%)**, and **consolidating tools (47%)**, reflecting a commitment to enhancing their capabilities to manage risk effectively.



Building on the previous findings, this shift toward risk-based strategies becomes an imperative tying together the need for better understanding of data risks, alignment between management and staff, and tools capable of addressing modern challenges. Risk-based strategies emphasize proactive vulnerability management, which not only reduces risks but also facilitates compliance as a secondary benefit.

Organizations must accelerate their transition to risk-based strategies to address evolving threats and growing complexities in their infrastructure and cloud environments. By prioritizing tools and processes that provide actionable insights, align with risk reduction priorities, and enhance operational efficiency, organizations can improve resilience while achieving compliance more efficiently. A risk-based approach enables organizations to stay ahead of vulnerabilities, align their investments with security outcomes, and navigate complex risk landscapes with confidence.

Final Thoughts on the State of Data Security Risk

The survey findings reveal clear steps organizations can take to strengthen their data security and risk posture management. First, they must **enhance their understanding of risks across hybrid and cloud environments** by leveraging tools and processes that provide actionable insights into high-risk data sources. This foundational step will close gaps in visibility and confidence, enabling more effective risk prioritization and mitigation.

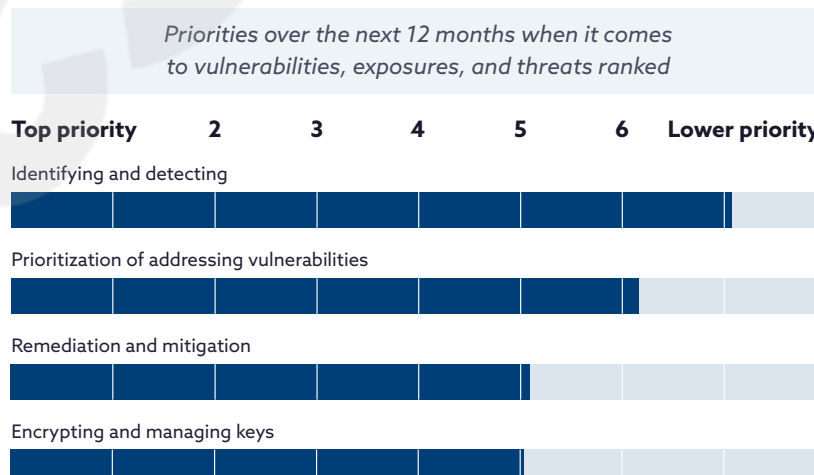
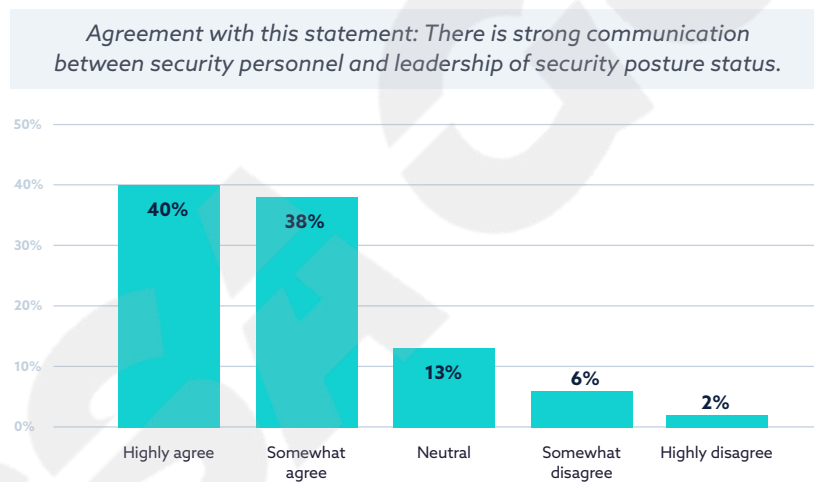
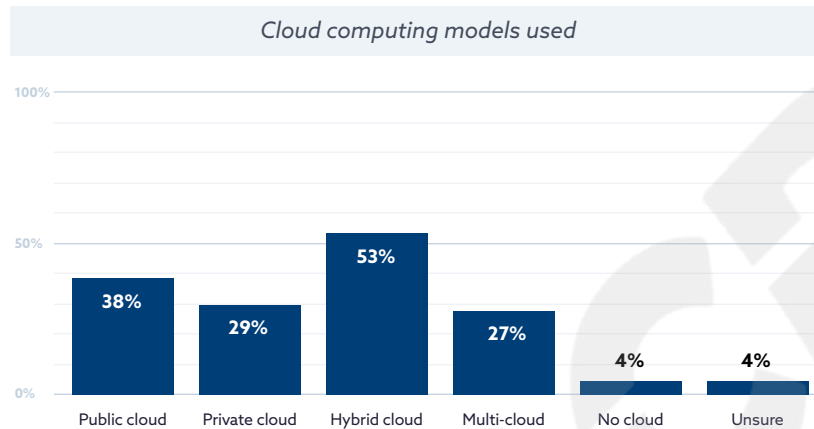
Second, organizations would benefit from **investing in unified platforms that integrate compliance, security, and risk management tools to address inefficiencies caused by siloed systems and tool proliferation**. Desired features in such platforms include assessment results, dedicated dashboard, and risk scores. Such platforms can streamline workflows, improve scalability, and align security efforts with broader business objectives.

Third, **better communication and collaboration between management and operational teams** is essential to align strategic goals with the realities of execution, ensuring organizations remain vigilant against emerging threats. Addressing resource constraints and ensuring operational needs are fully supported will bridge existing gaps and improve the effectiveness of risk strategies.

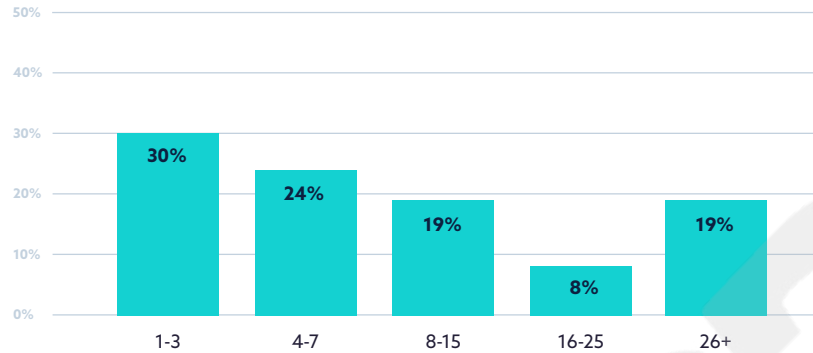
Lastly, organizations must **shift toward proactive, risk-based approaches** that prioritize dynamic risk evaluation, vulnerability management, and adaptability—allowing them to confidently reduce the risk of evolving threats. By doing so, they can not only strengthen their resilience but also achieve compliance as a natural outcome of robust data protection and security practices. Together, these actions provide a clear roadmap for navigating today's complex risk landscape and protecting critical data assets.

Full Survey Results

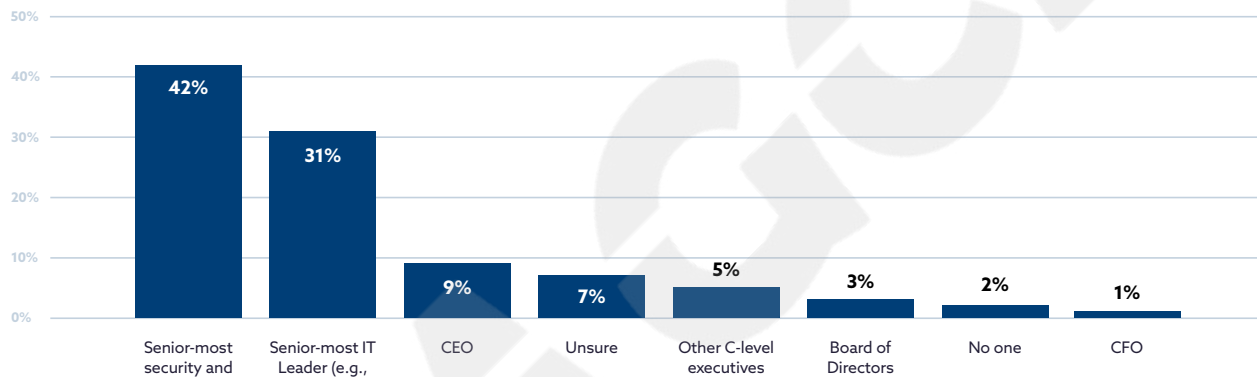
Overview



Number of individuals per organization that are involved in risk identification and remediation

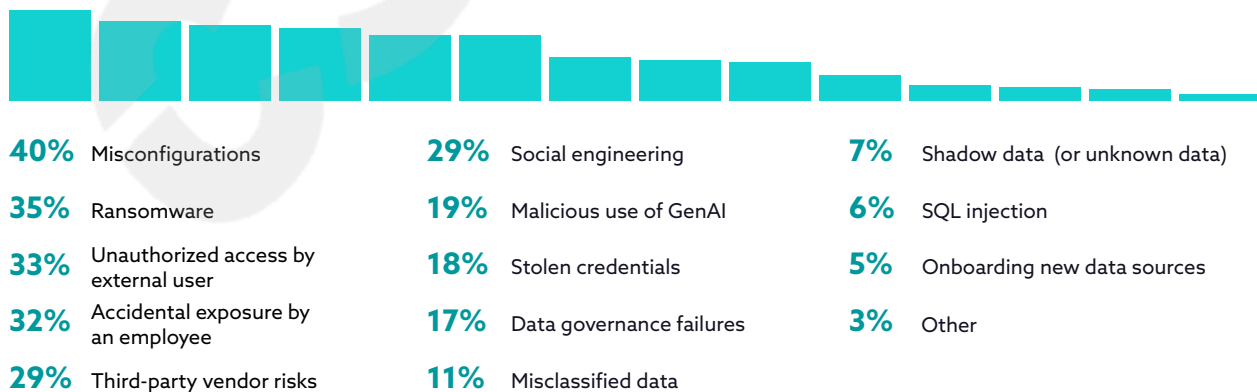


Person primarily held accountable for a data security incident

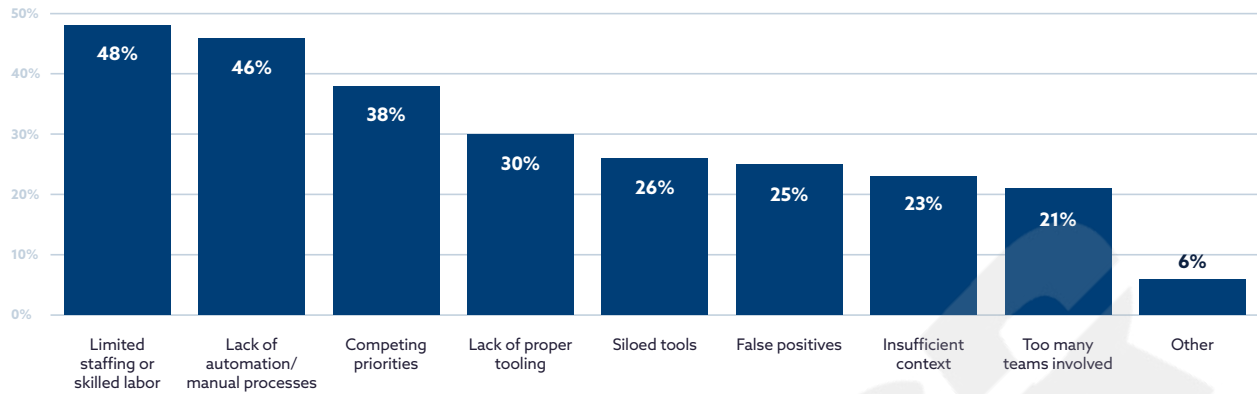


Concerns and Challenges

Data risk incidents organizations' are most concerned about over the next 12 months

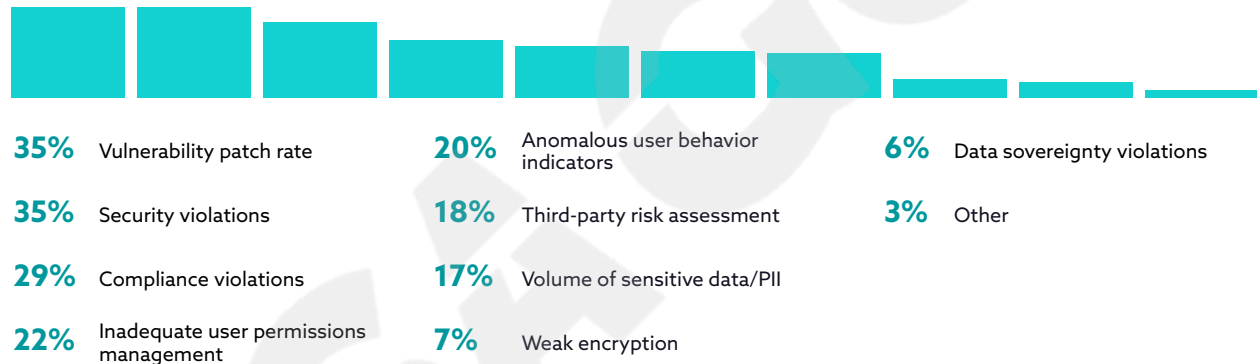


Top challenges when identifying risk in organizations' data infrastructure



Risk Evaluation Strategy

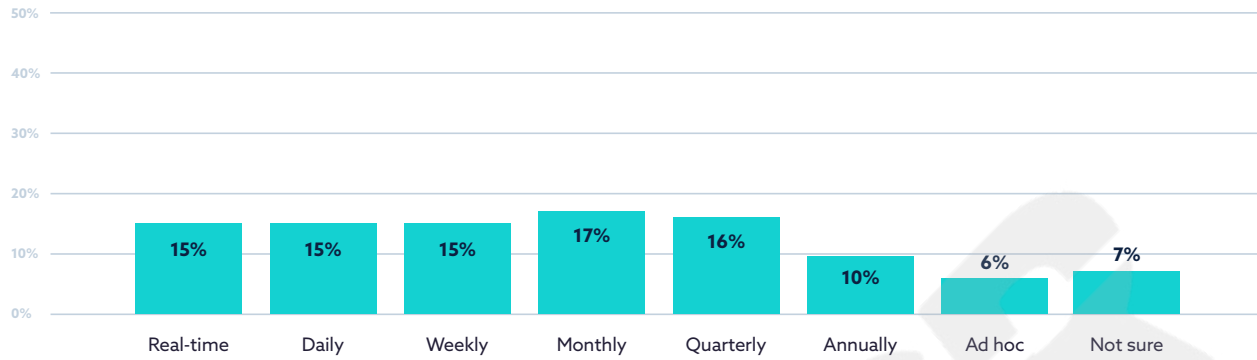
Key risk indicators organizations use



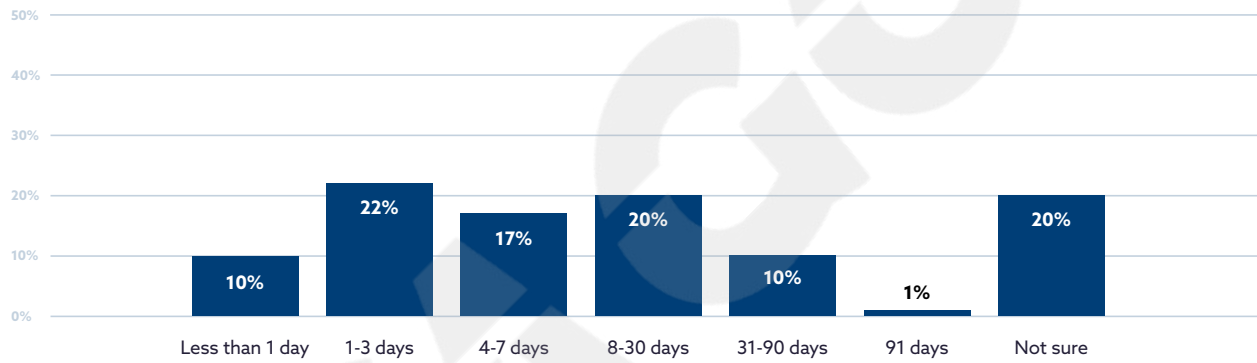
Most helpful features for understanding organizations' data risk



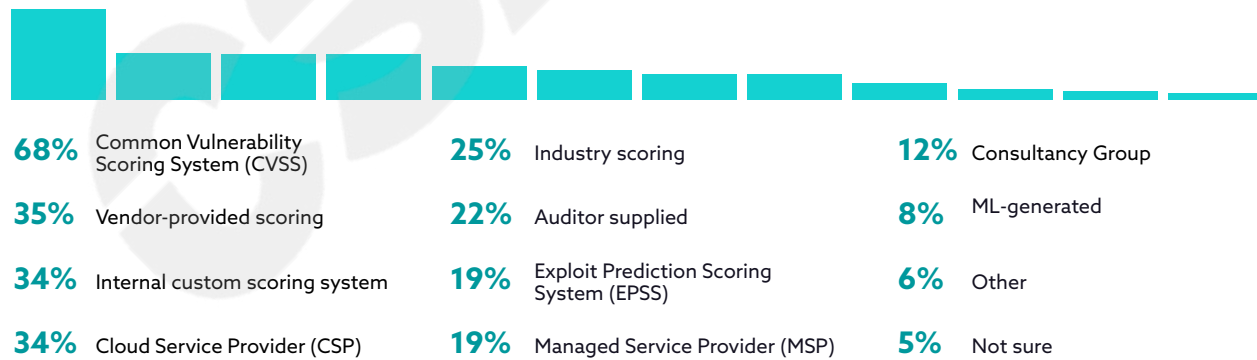
Frequency of evaluating cybersecurity risk across different business units and critical assets



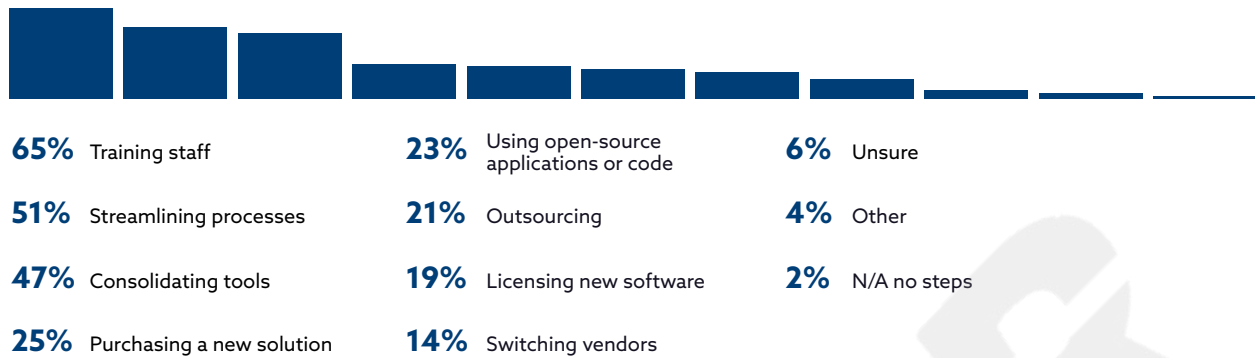
Length of cybersecurity risk evaluations across different business units and critical assets



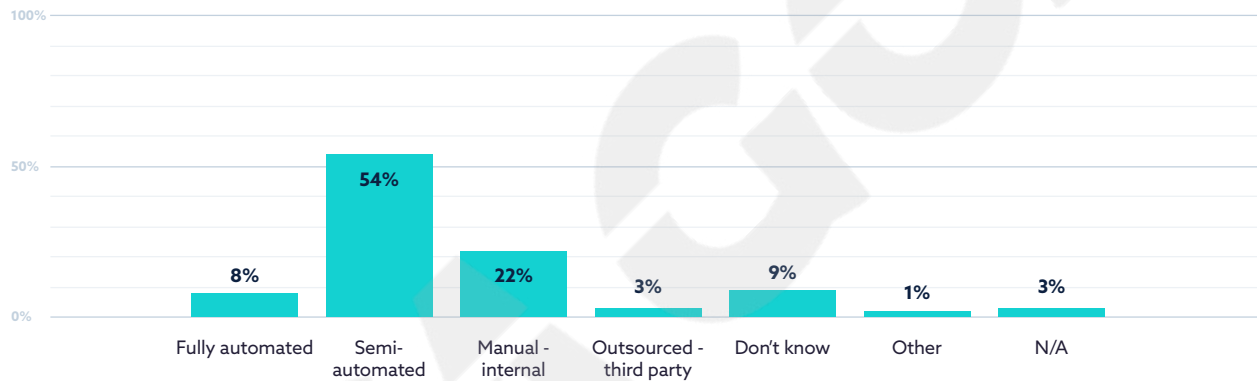
Risk-sharing approach used to assess the severity of vulnerabilities



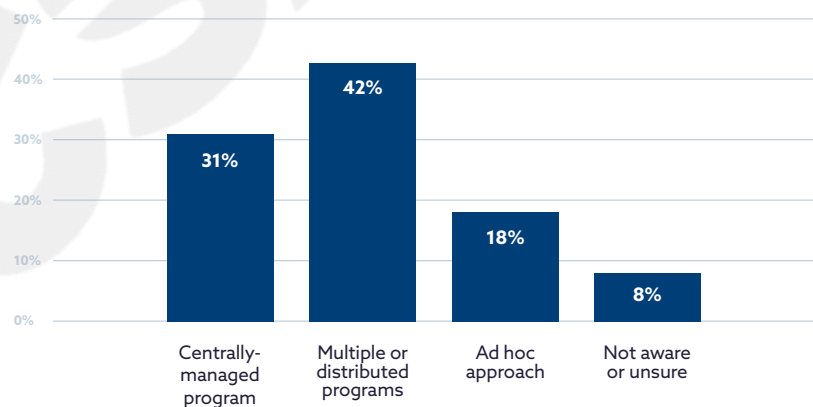
Activities utilized to maximize the value of risk management budgets



Level of automation to evaluate risk for data repositories, data lakes, and cloud services across assets, business units, and locations

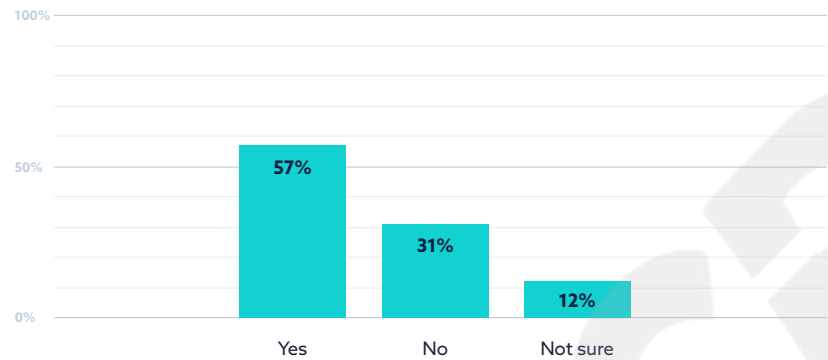


Hybrid Environments Users Only - Type of program used process across environments for managing data exposure and investigating risk?

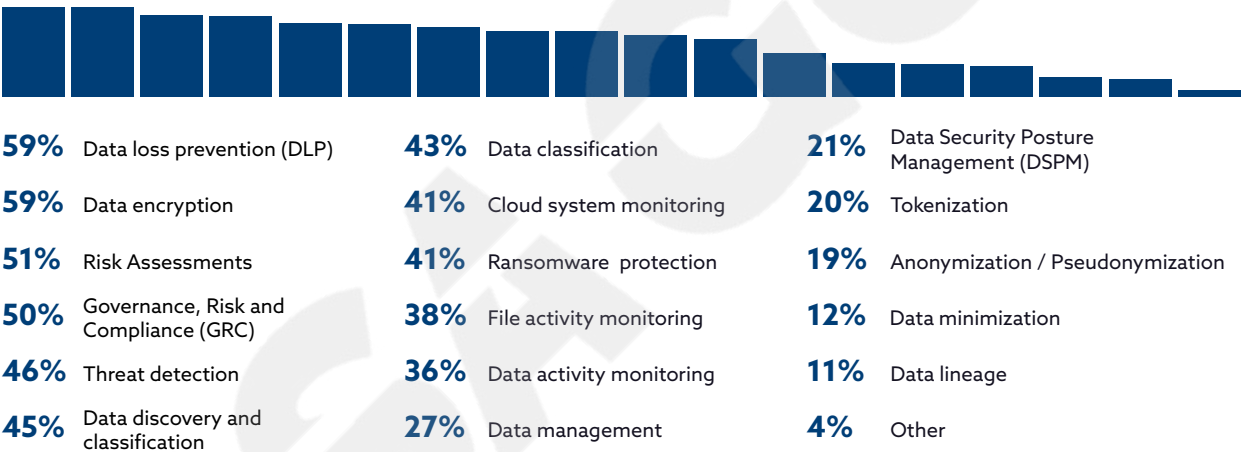


Risk Management Tools

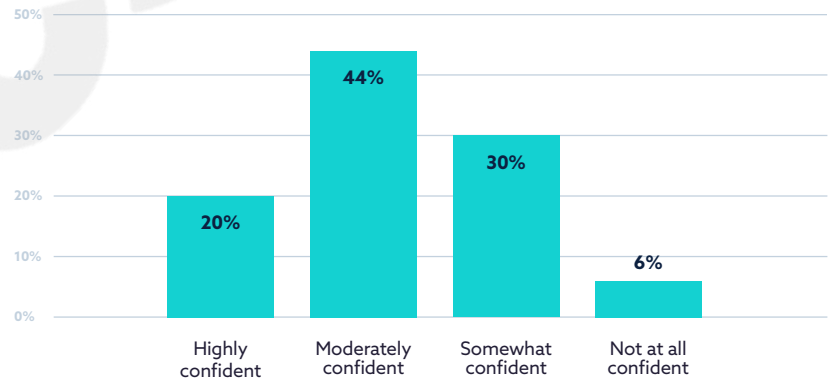
Tool to identify the number of data sources (e.g., databases, cloud storage) that are riskiest



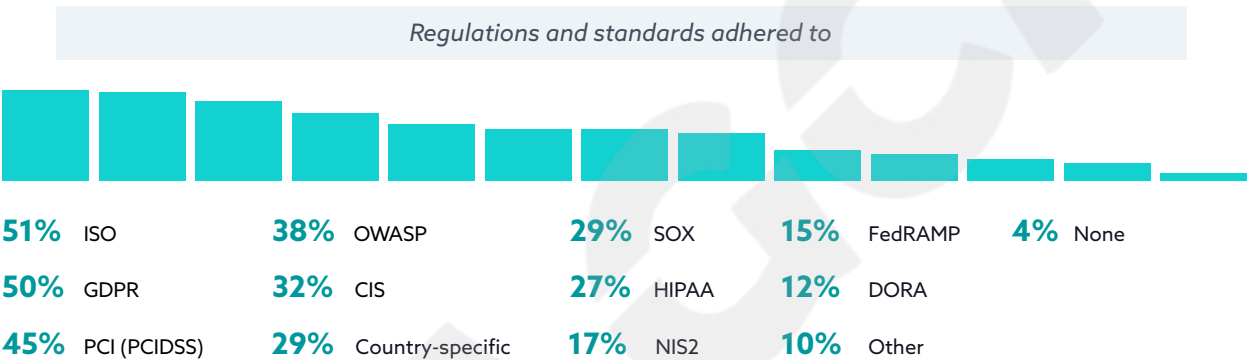
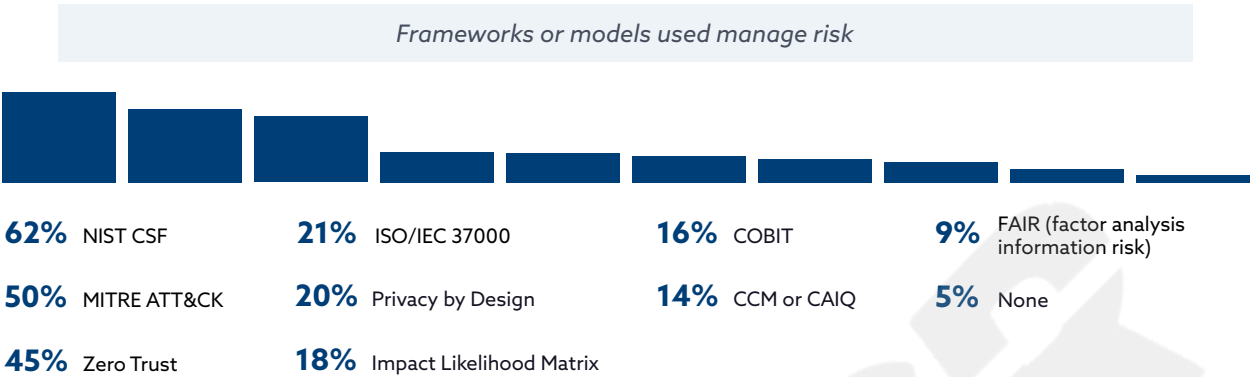
Tools used to manage data risk



Confidence in ability to identify high-risk data sources



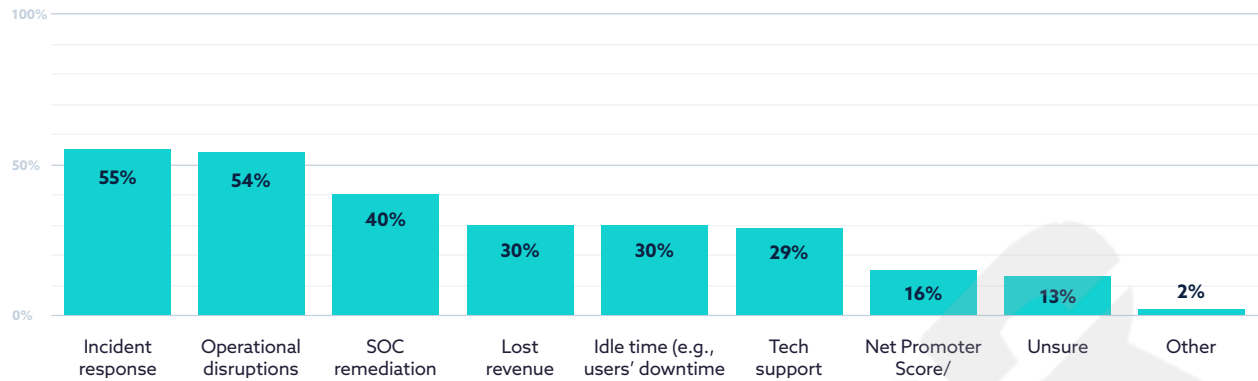
Compliance and Standards



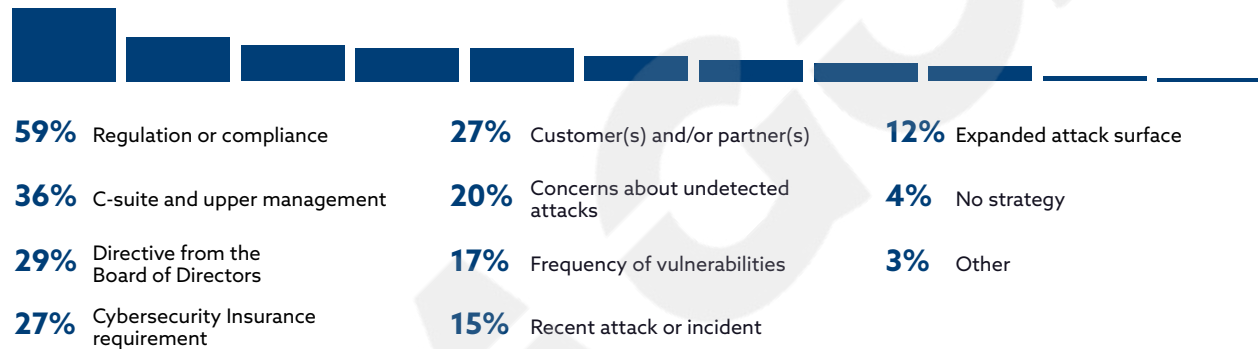
Program Strategy and Drivers



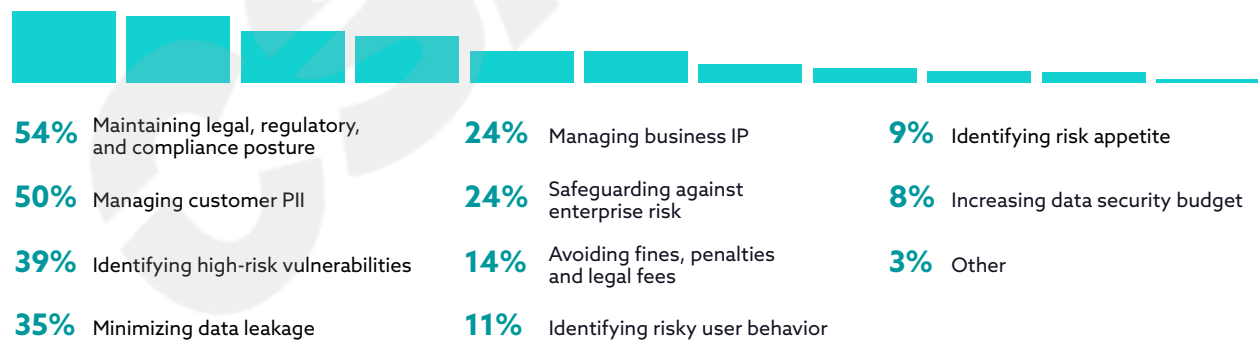
KPIs CISOs use to translate cybersecurity risk into financial terms



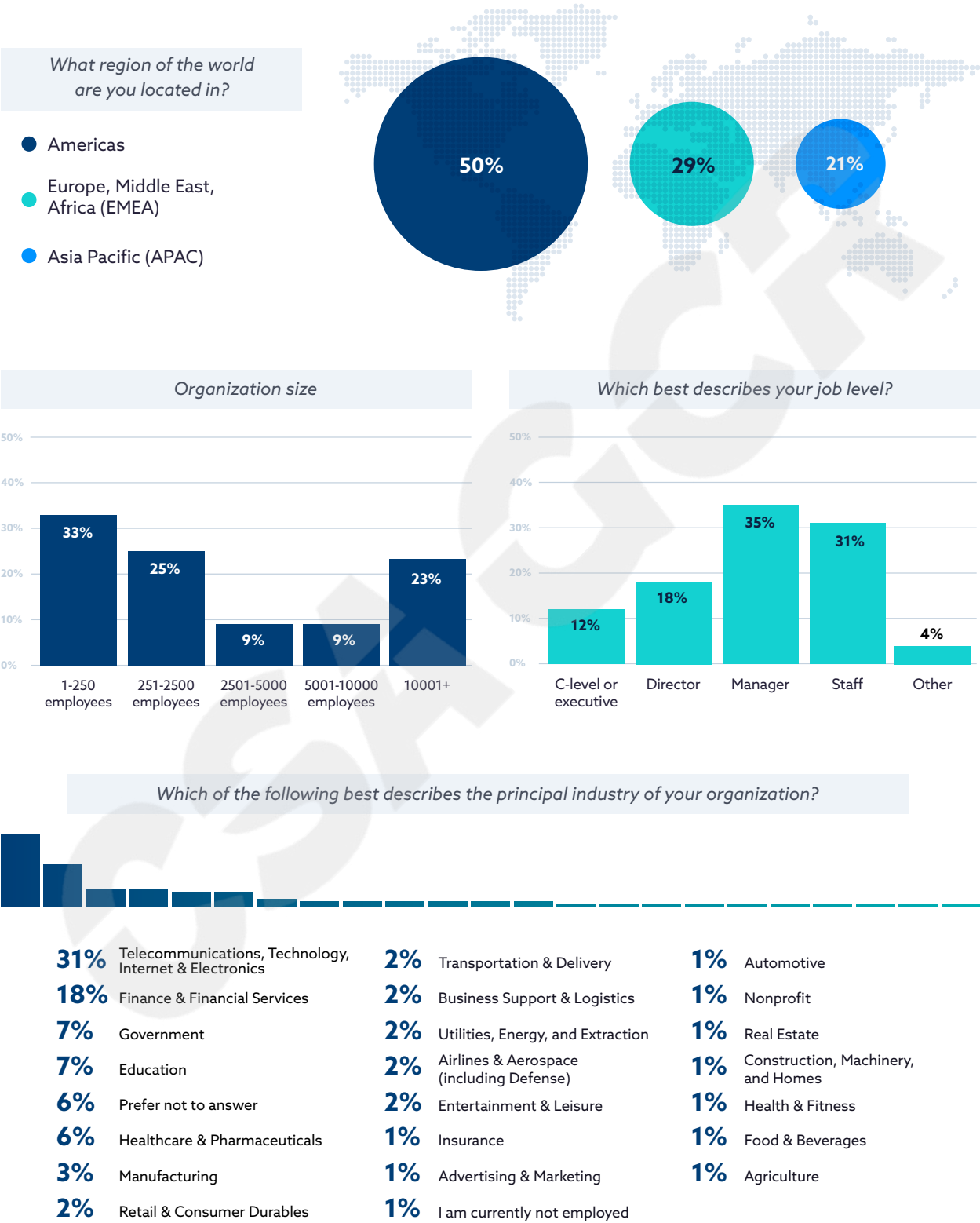
Main drivers for data risk reduction strategy



Top focus areas for data risk



Demographics



Survey Methodology and Creation

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices and ensure cybersecurity in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Thales commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding data risk security and its challenges. Thales financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in November 2024 and received 912 responses from IT and security professionals from organizations of various sizes and locations. CSA's research analysts performed the data analysis and interpretation for this report.

Goals of the Study

This survey aims to provide a comprehensive understanding of how organizations assess and manage cybersecurity and data risks. By examining current practices, tools, and strategies, it seeks to evaluate the effectiveness of data security evaluation methods and highlight areas for improvement. Specifically, the survey focuses on:

- **Methods for Assessing Data Risk:**
Understanding how organizations identify, categorize, and evaluate risks across their data assets, including on-premises, hybrid, and cloud environments.
- **Tools and Automation for Risk Evaluation:**
Exploring the tools organizations rely on to monitor, assess, and mitigate risks, with an emphasis on automation and its role in enhancing efficiency and reducing manual processes.
- **Challenges and Priorities in Risk Evaluation:**
Identifying key obstacles organizations face in evaluating risks, such as resource limitations, siloed tooling, and operational inefficiencies, as well as understanding their top priorities for improvement.

Cloud Security Alliance Greater China Region



扫码获取更多报告