2024 STATE OF HEALTHCARE

Cloud Security and Compliance Posture Report

CLEARDATA®

healthcare innovation
PEOPLE. PROCESS. TECHNOLOGY TRANSFORMATION.®

TABLE OF CONTENTS

Executive Summary **3**

Introduction: Charting the Course for Healthcare Security and Compliance **4**

Current State & Confidence Levels **5**
Cloud Trios Dominate Healthcare IT 5
Cybersecurity Challenges Stall Cloud Use 6

Top Concerns & Preparedness Tactics **8**
Amid Variety of Security Concerns, Misconfigurations Overlooked 8
Are Data Breach Fears and Readiness Out of Sync? 11
Constant Wave of Cyber Threats 12

Approaches to Management & Software Solutions **13**
Balanced Approach to Cybersecurity and Compliance 13
Cost Takes Backseat When Choosing Solutions 14
Compliance Outweighs Patient Safety 15

Budget Trends & Future Planning **16**
Spending Is Increasing 16
Staffing and Tech Drive Spending 19

How to Futureproof Healthcare Cloud Security & Compliance Posture **20**
Actionable Takeaways for Healthcare Leaders 20

Conclusion: Forging Ahead in Healthcare Security and Compliance **21**
About the Survey 21

EXECUTIVE SUMMARY

Healthcare cyberattacks surged 136% in this past year, a troubling trend that shows no signs of slowing down. To understand how healthcare leaders are responding, ClearDATA surveyed nearly 200 healthcare technology professionals in leadership positions. Most work within a healthcare provider organization's IT department and hold managerial or executive roles, with nearly half reporting annual revenues exceeding $500 million.

These leaders answered questions about the state of their security and compliance posture, funding priorities, top concerns, and more. And the results are sobering. Despite a clear and present danger, healthcare IT may be overestimating their organization's preparedness to detect and respond to cyberattacks. Cybersecurity and compliance budgets and training are increasing, yet misconfigurations remain a persistent problem — nearly 80% reported at least one last year — and only 23% of organizations are using multi-factor authentication (MFA), a basic yet critical defense against breaches like the devastating Change Healthcare attack in February. Among the nearly 1,000 hospitals surveyed by the American Hospital Association, 74% reported patient care disruptions, and 94% faced financial hardships.

Nonetheless, we also see progress, with many respondents prioritizing improvements to threat detection and response, and tech upgrades. Cloud maturity levels are also growing. But preparedness gaps remain.

These findings underscore the urgent need for a shift in mindset and approach to healthcare cybersecurity. Fortunately, effective solutions exist. By taking decisive action, healthcare organizations can significantly enhance their security posture and protect themselves and their patients.

Chris Bowen, ClearDATA Founder and CISO

INTRODUCTION: Charting the Course for Healthcare Security and Compliance

With healthcare cyber threats more frequent and sophisticated, organizations cannot afford to fall behind on security and compliance measures. This report sheds light on the current state of healthcare cloud security, highlighting where we excel, where we stumble, and how we can improve.

Budget constraints, data management, and cyberattacks are the biggest challenges, but the data also indicates a notable gap between managers' and executives' perceptions of security readiness and often-overlooked risks like cloud misconfigurations. The report also outlines IT budget allocations amid rising cybersecurity costs and a trend toward hybrid solutions and increased training and staffing. However, the data shows staff training alone still leaves healthcare leaders grappling with persistent attacks, underscoring the urgent need for proactive, expert strategies.

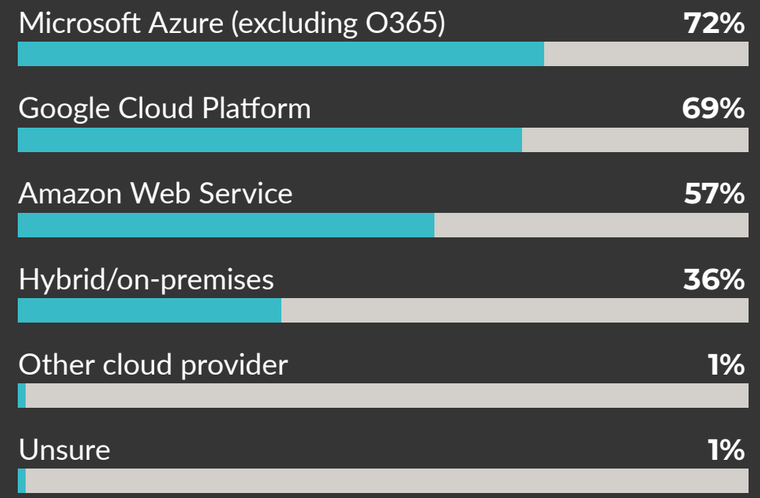
To protect patient privacy and organizational integrity, we encourage health tech leaders to share these findings and actionable advice with others in their organizations to optimize resources and better tackle the threats.

Cloud Trios Dominate Healthcare IT

Microsoft Azure, Google Cloud, and Amazon Web Services are the most frequently used cloud platforms. The top three reasons for cloud use are data analytics, patient portals, and EHR/EMR software. The prioritization of data analytics signals a growing emphasis on data-driven decision-making, while patient portals and cloud-based EHR/EMR reflect a broader trend toward patient-centered care and convenience. As sensitive patient data migrates to the cloud, adopting robust security measures is critical, especially as the interconnected nature of these platforms means vulnerabilities in one area can cascade, potentially exposing multiple aspects of an organization's operations.

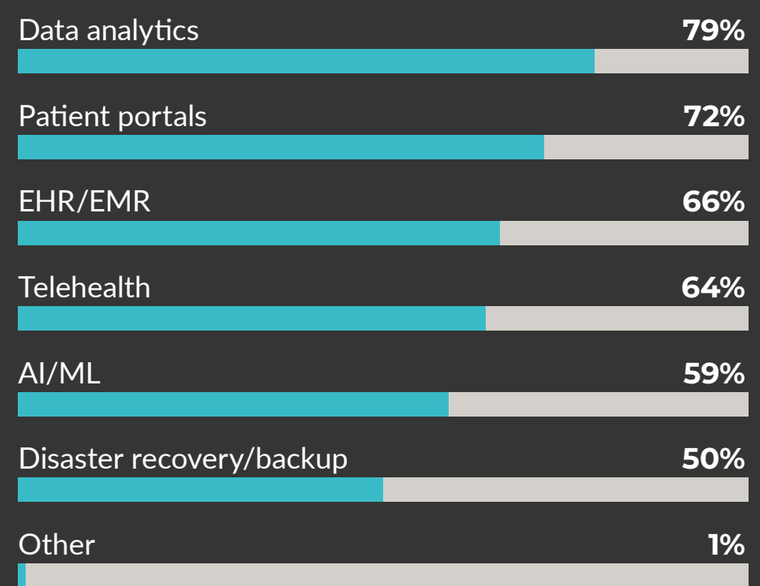
Which public or private cloud infrastructure platforms does your organization leverage?

Base: Foundational, intermediate and advanced respondents (n=152). Multiple answers allowed.



What types of workloads is your organization utilizing the cloud for?

Base: Private and public cloud platform users (n=152). Multiple answers allowed.

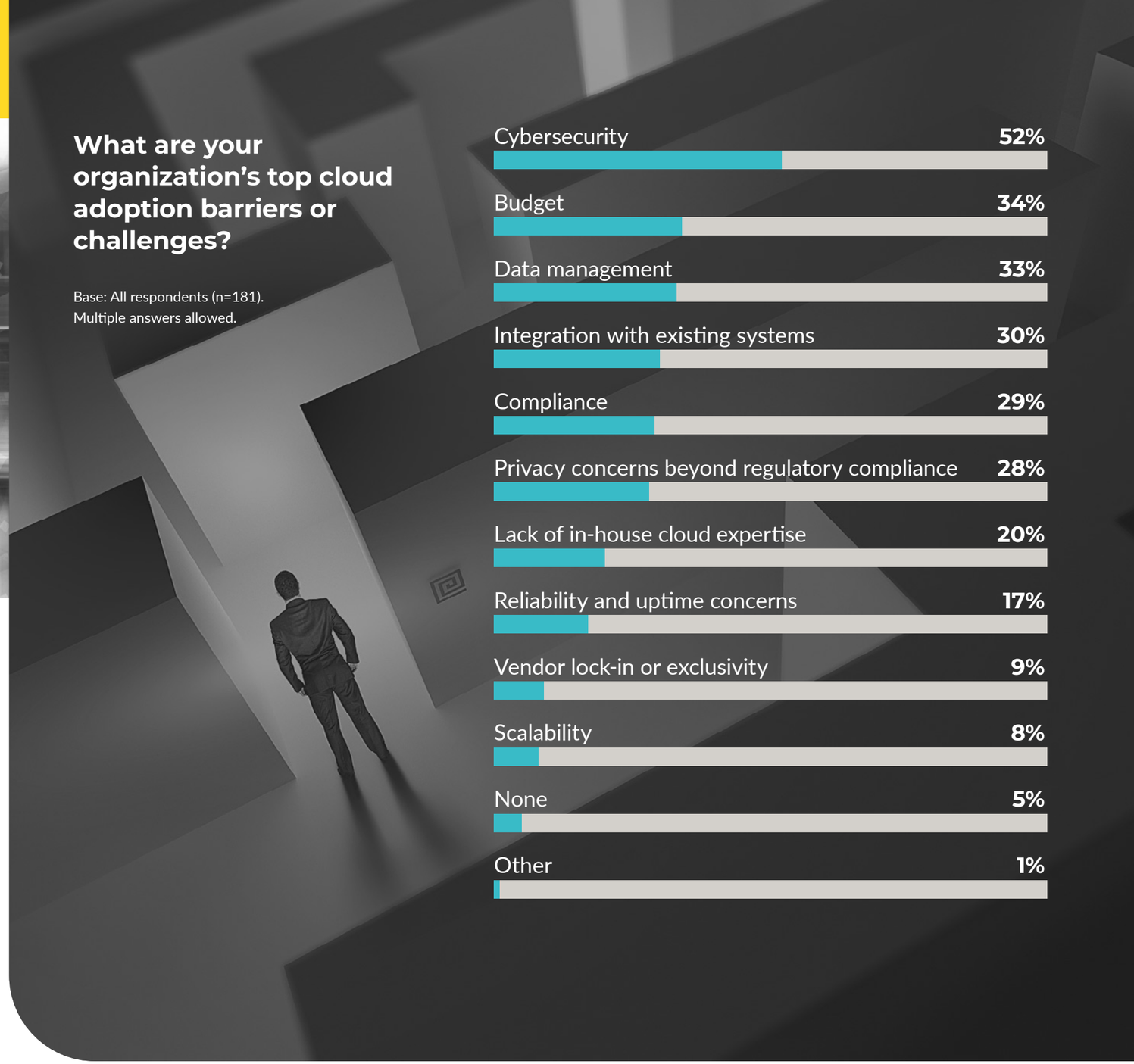


Cybersecurity Challenges Stall Cloud Use

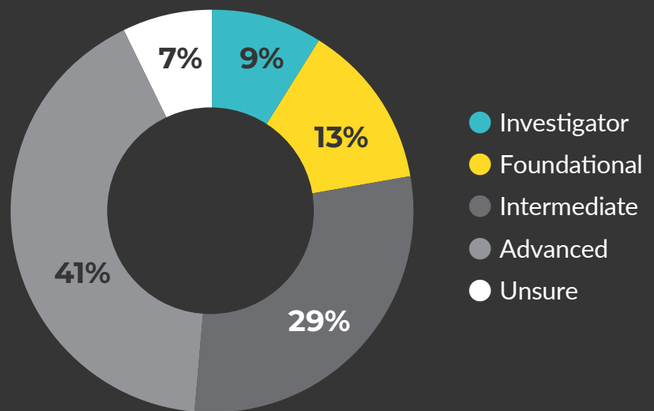
Cybersecurity, the primary barrier to cloud adoption, underlines significant concerns surrounding data protection, which may indicate uncertainty or caution about migrating to the cloud. Budget constraints and data management challenges further emphasize the complexities of cloud adoption. The potential benefits of cloud computing are substantial, but the initial investment and ongoing costs can be prohibitive for some healthcare organizations. Additionally, effectively managing data within a cloud environment requires specialized expertise and resources, which 20% of respondents lack.

What are your organization's top cloud adoption barriers or challenges?

Base: All respondents (n=181).
Multiple answers allowed.

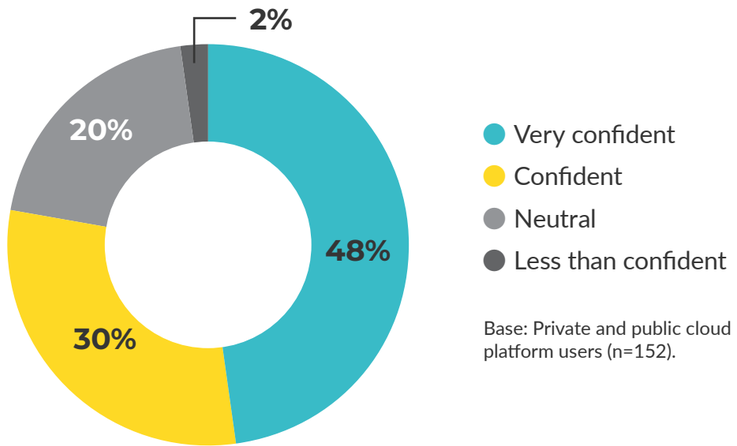


What's your organization's cloud maturity level?



Base: All respondents (n=181).

How confident are you in the security and compliance program you currently have in place to protect the sensitive data/protected health information (PHI) your organization stored in the cloud?

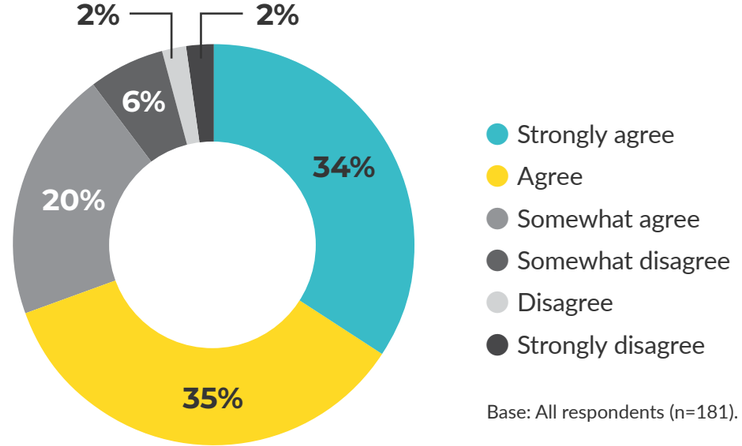


Base: Private and public cloud platform users (n=152).

Confidence Levels in Cloud Security and Compliance Are on the Rise

Most respondents see their organization's cloud maturity as intermediate or advanced, which suggests they're building a solid foundation. Cloud users also expressed high confidence in their current security and compliance programs. Interestingly, C-level executives were much more likely than others to describe their maturity level as advanced, a disparity that suggests gaps in strategic perspective and operational execution.

To what extent do you agree or disagree with this statement: Our security and compliance teams operate as a single unit with shared goals and responsibilities.

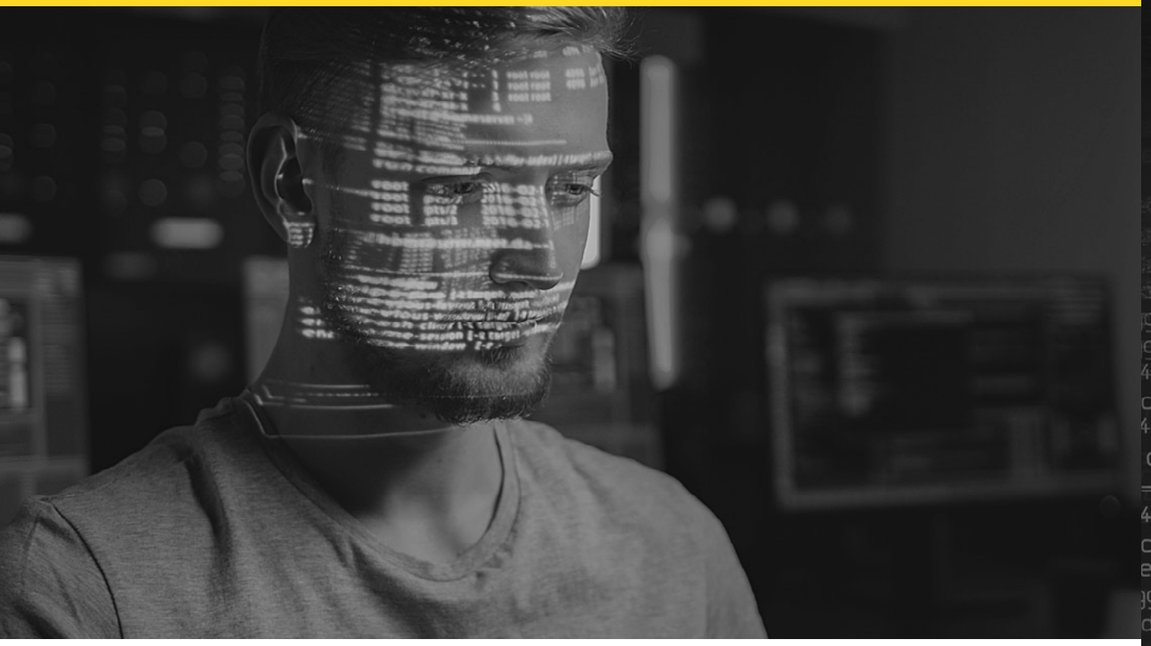


Base: All respondents (n=181).

Strong Alignment Between Security and Compliance Teams

Most respondents believe their security and compliance teams are unified with shared objectives, indicating the importance of collaboration. Though a small percentage operate separately, pointing to potential areas for improvement, the overall trend is an integrated approach to security and compliance.

TOP CONCERNS & PREPAREDNESS TACTICS

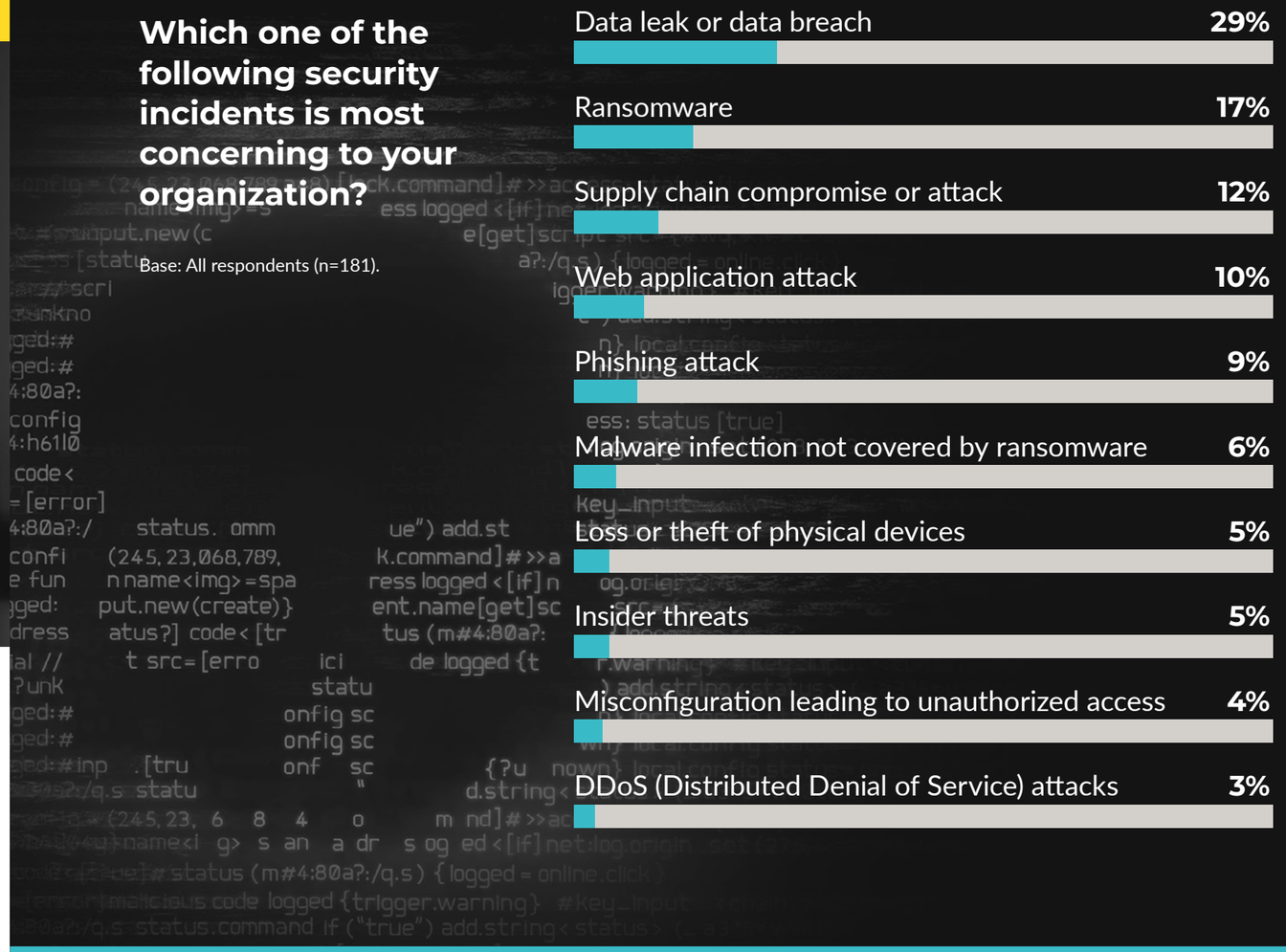


Misconfigurations Overlooked Amid Security Concerns

Data leaks/breaches remain the top security concern, followed by ransomware and supply chain compromises. While these issues command significant attention, low concern about misconfigurations is surprising, given their potential for severe consequences. According to an XM Cyber report, 80% of security incidents are caused by misconfigurations, and one-third of them put critical assets at risk. Misconfigurations provide entry points for cyberattacks and other incidents which can be costly to remediate, underscoring potentially catastrophic security gaps healthcare must address.

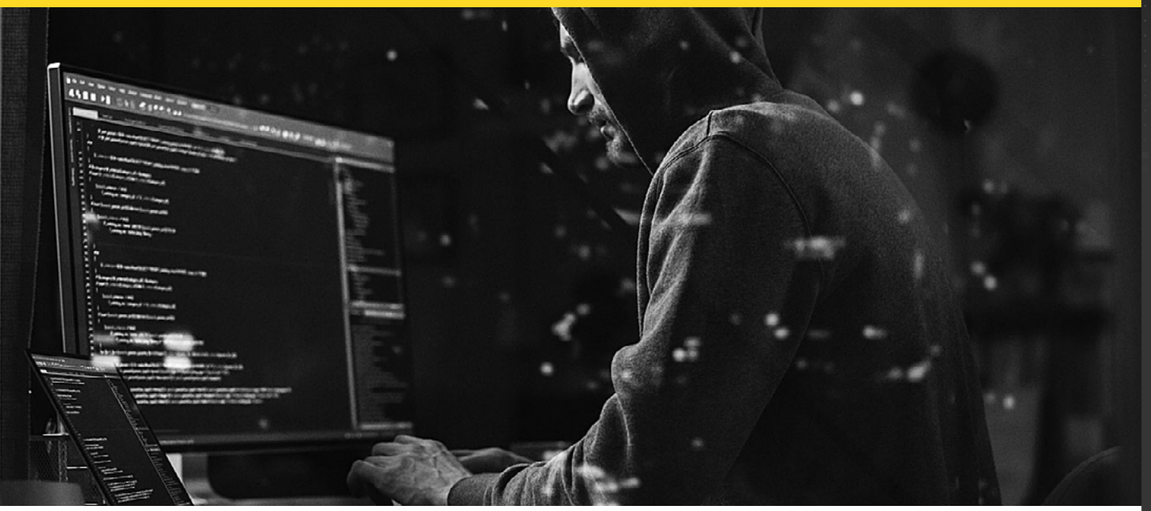
Which one of the following security incidents is most concerning to your organization?

Base: All respondents (n=181).



80% of security incidents are caused by misconfigurations, yet only 4% of respondents are concerned about them.

TOP CONCERNS & PREPAREDNESS TACTICS



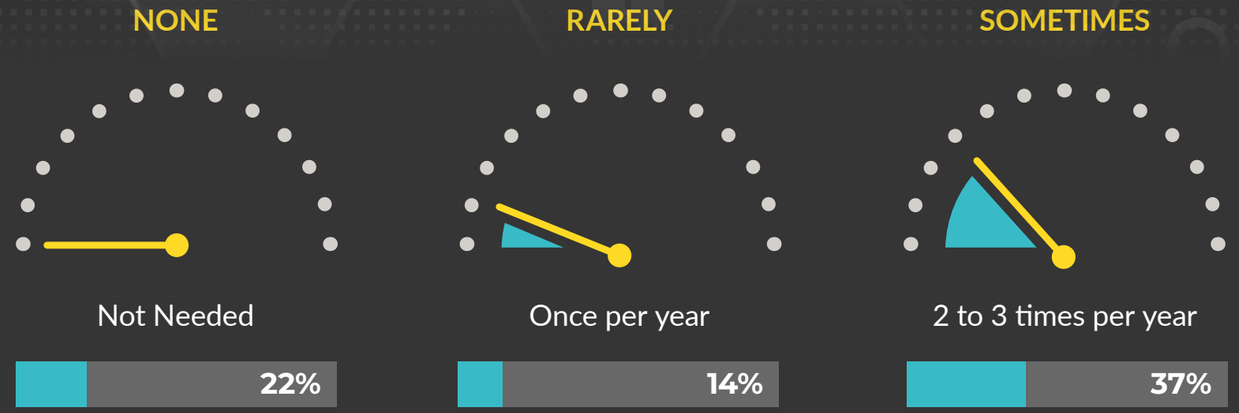
Cloud Misconfigurations Are Common, Impacts Severe

More than a third of organizations remediated multiple cloud misconfigurations in the past year, stressing the ongoing struggle healthcare has maintaining secure cloud environments and need for robust cloud security practices. Remediations are not only time-consuming but can cost tens of millions annually. The financial burden and operational disruptions caused by misconfigurations lead to significant downtime, loss of revenue, and damage to an organization's reputation.

"The prevalence of misconfigurations — a root cause of data breaches — is alarming. Seemingly minor configuration errors, whether an issue with MFA, a patch that wasn't applied, or an issue with an encryption algorithm, can devastate healthcare systems."

— Chris Bowen, ClearDATA Founder and CISO

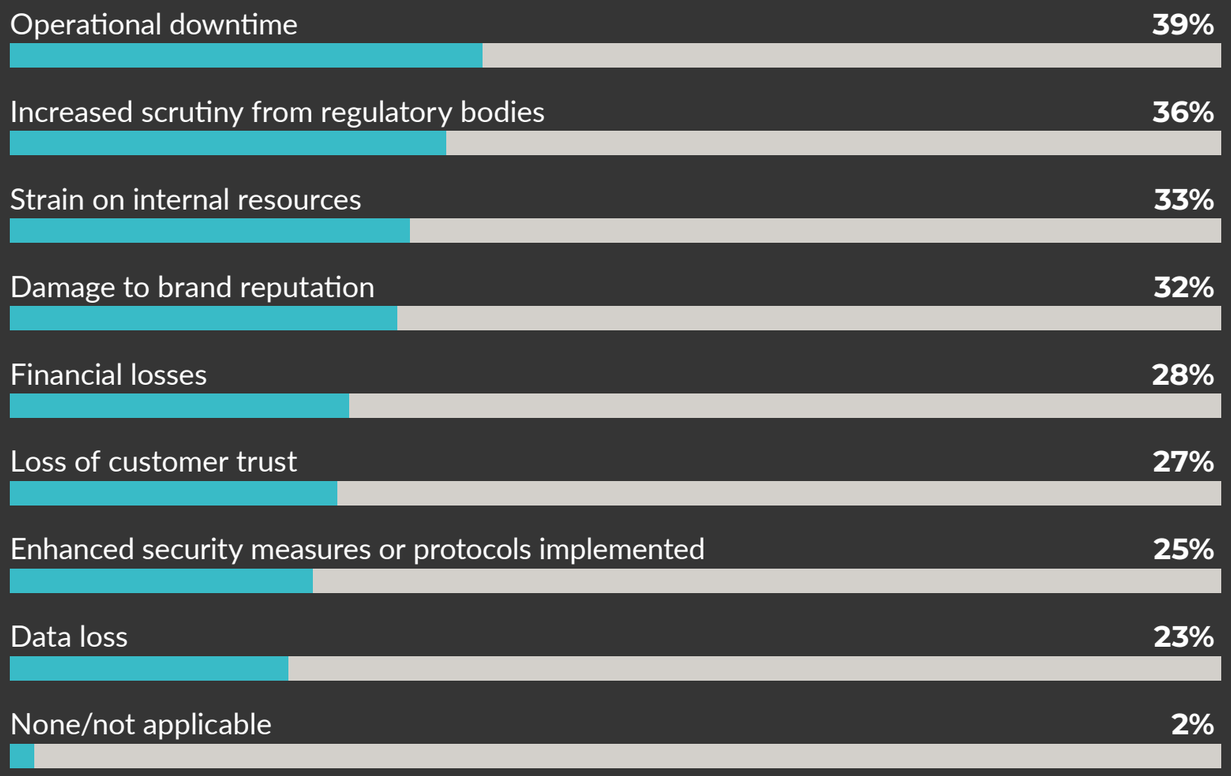
How many cloud misconfigurations did your organization have to remediate in the last 12 months?



Base: All respondents (n=181).

TOP CONCERNS & PREPAREDNESS TACTICS

What were the most significant impacts your organization experienced due to cloud misconfigurations?

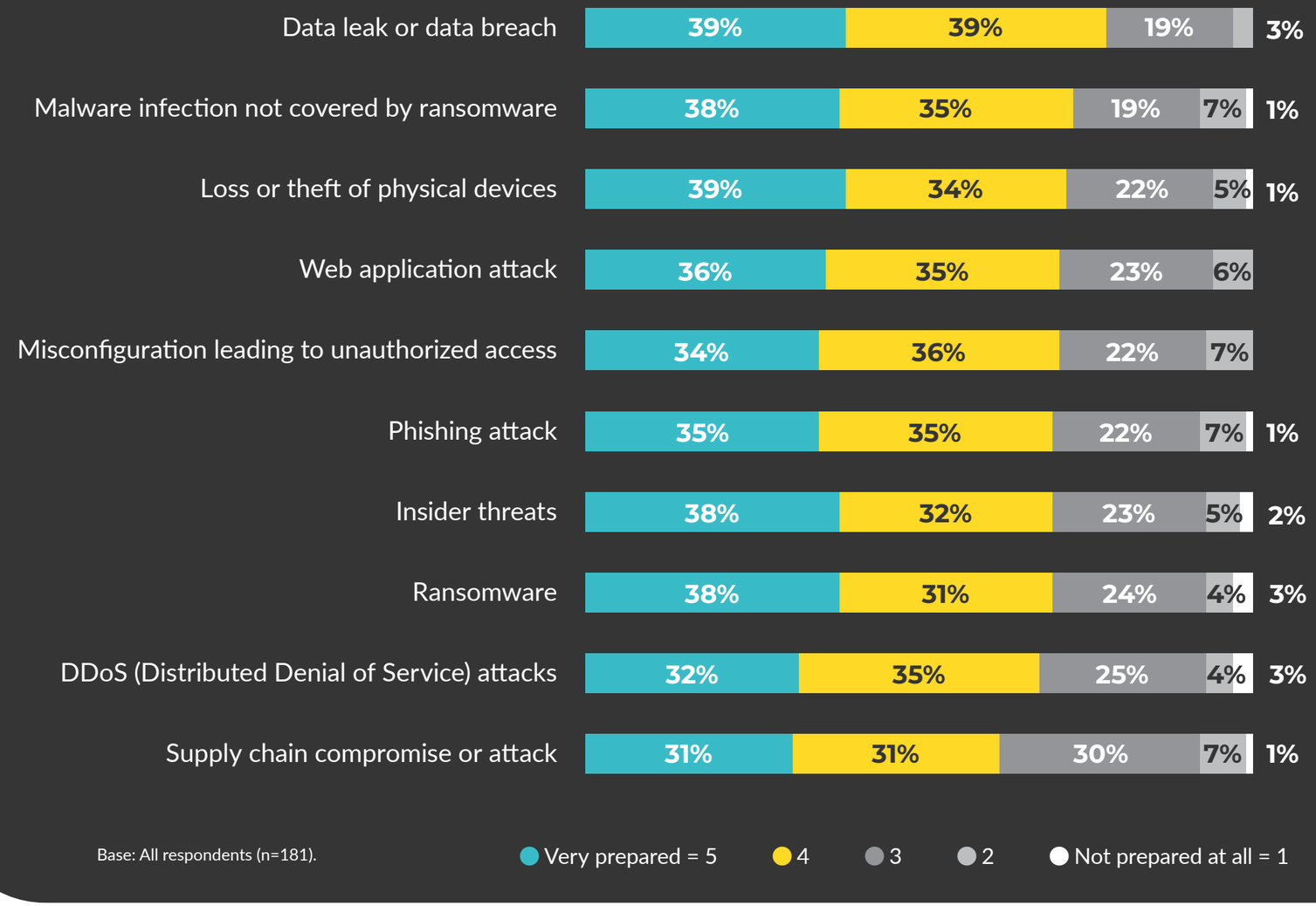


Base: Respondents with cloud misconfigurations (n=142).
Multiple answers allowed.

Are Data Breach Fears and Readiness Out of Sync?

Despite high concern about data leaks or breaches, most respondents feel confident in their organization's preparedness to manage them. The discrepancy between concern and confidence suggests a potential gap in understanding or a mismatch between perception and reality. Healthcare organizations may be implementing security measures but underestimating the complexity and sophistication of modern cyberattacks. A comprehensive threat assessment would help identify vulnerabilities and prioritize mitigation efforts.

How confident are you in your organization's preparedness to handle each of the following security incidents?



Base: All respondents (n=181).

CLEARDATA®

healthcare innovation
PEOPLE, PROCESS, TECHNOLOGY TRANSFORMATION.®

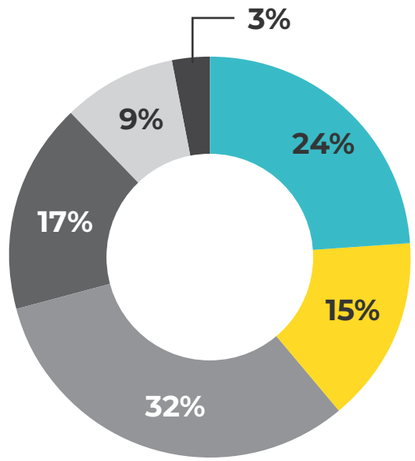
TOP CONCERNS & PREPAREDNESS TACTICS

Constant Wave of Cyber Threats

With most respondents reporting two to three cyber incidents/breaches within the past year, organizations recognize the need to be proactive, not reactive. The parallel emphasis on compliance also indicates a growing awareness of the regulatory requirements and potential liabilities associated with breaches.

How many cyber incidents or IT security related breaches has your healthcare organization experienced in the last 12 months?

Base: All respondents (n=181).



76% of all respondents faced at least one security incident in the last year and 29% experienced 4 or more.

Which of the following are your organizations' cybersecurity priorities?

Base: All respondents (n=181).
Multiple answers allowed.

Balanced Approach to Cybersecurity and Compliance

Nearly half of respondents with advanced cloud maturity levels employ a hybrid approach to cybersecurity and compliance, combining in-house and outsourced capabilities. This approach allows organizations to leverage the specialized skills of vendors to manage the complexities, resource demands, and complex regulatory landscape.

DIY versus Outsourcing

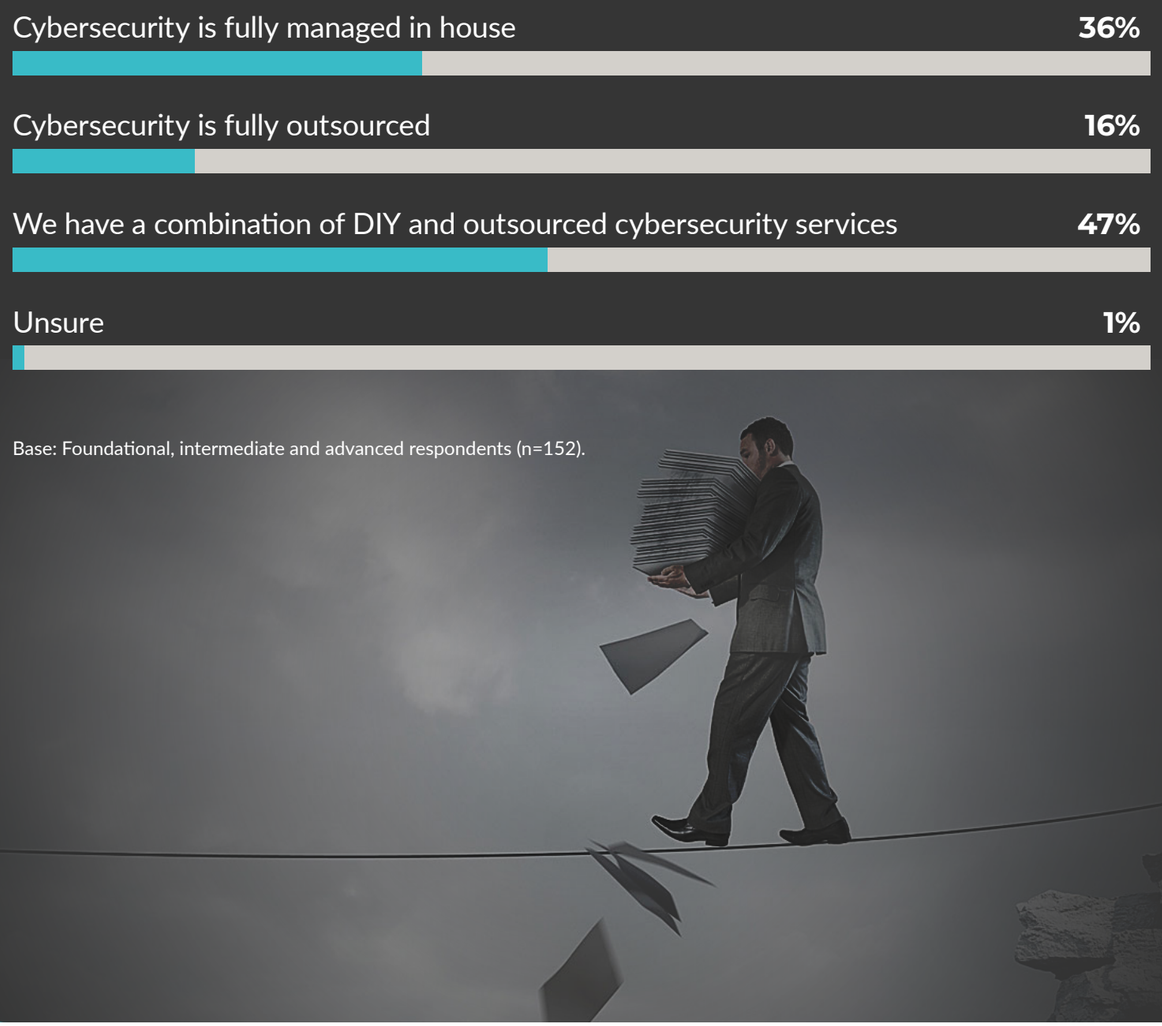
Building an advanced cybersecurity team in-house is challenging. In addition to the salary, training, certifications, benefits, and other costs required, there is a shortage of cybersecurity talent, particularly those with healthcare-specific knowledge and expertise.

Beyond direct costs, consider the qualitative factors of partnering with a third party:

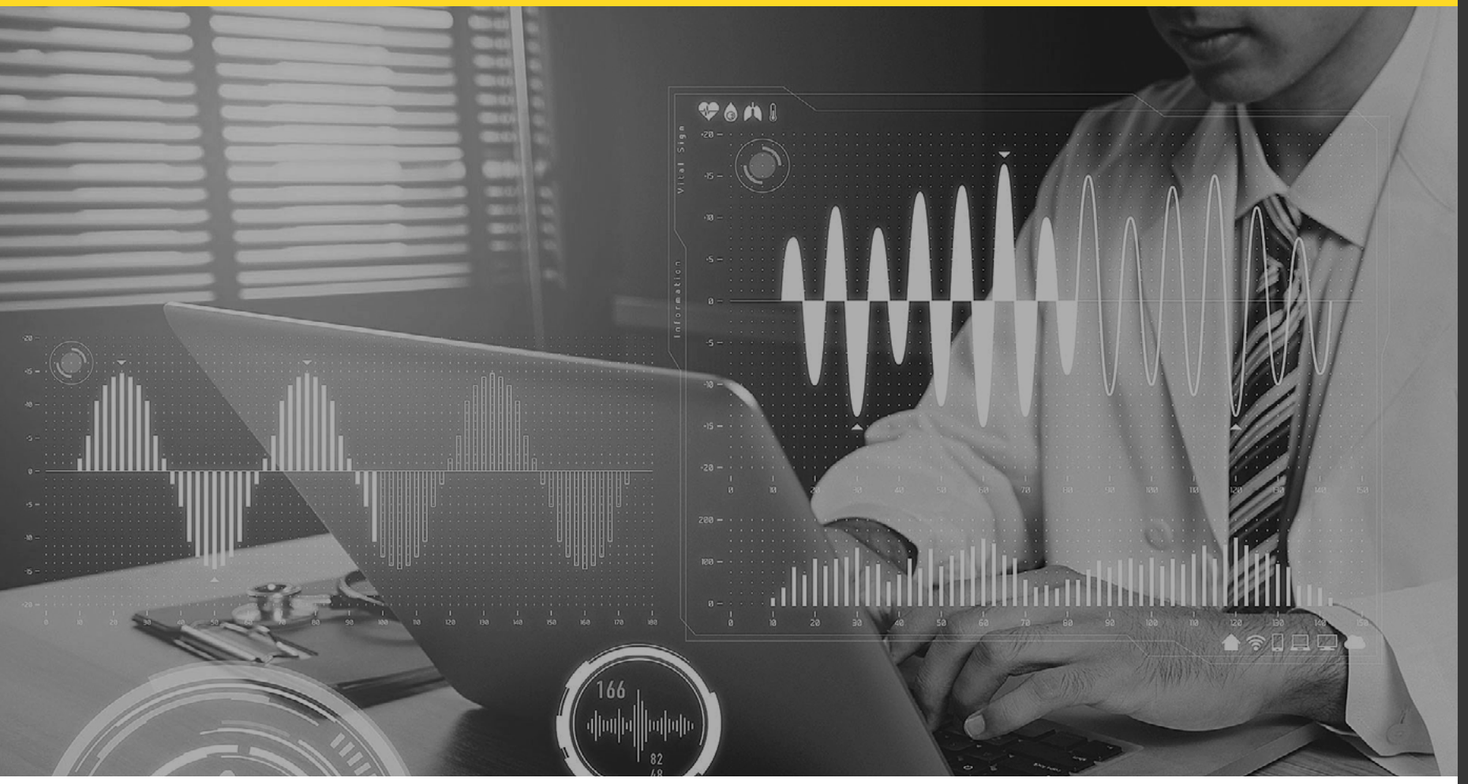
- **EXPERTISE:** Third-party providers often have specialized expertise and access to the latest threat intelligence.
- **SCALABILITY:** Third-party services can be more scalable to accommodate fluctuations in security needs.
- **COMPLIANCE:** Some regulations might mandate healthcare-specific security controls, which might be easier to achieve with a third-party provider.
- **FOCUS:** In-house teams might be diverted from core healthcare operations, while third-party providers specialize in cybersecurity.

Source: 2023 HIMSS Healthcare Cybersecurity Survey Report

Does your organization manage security with a (DIY) platform and approach, or do does it outsource security measures in the cloud?



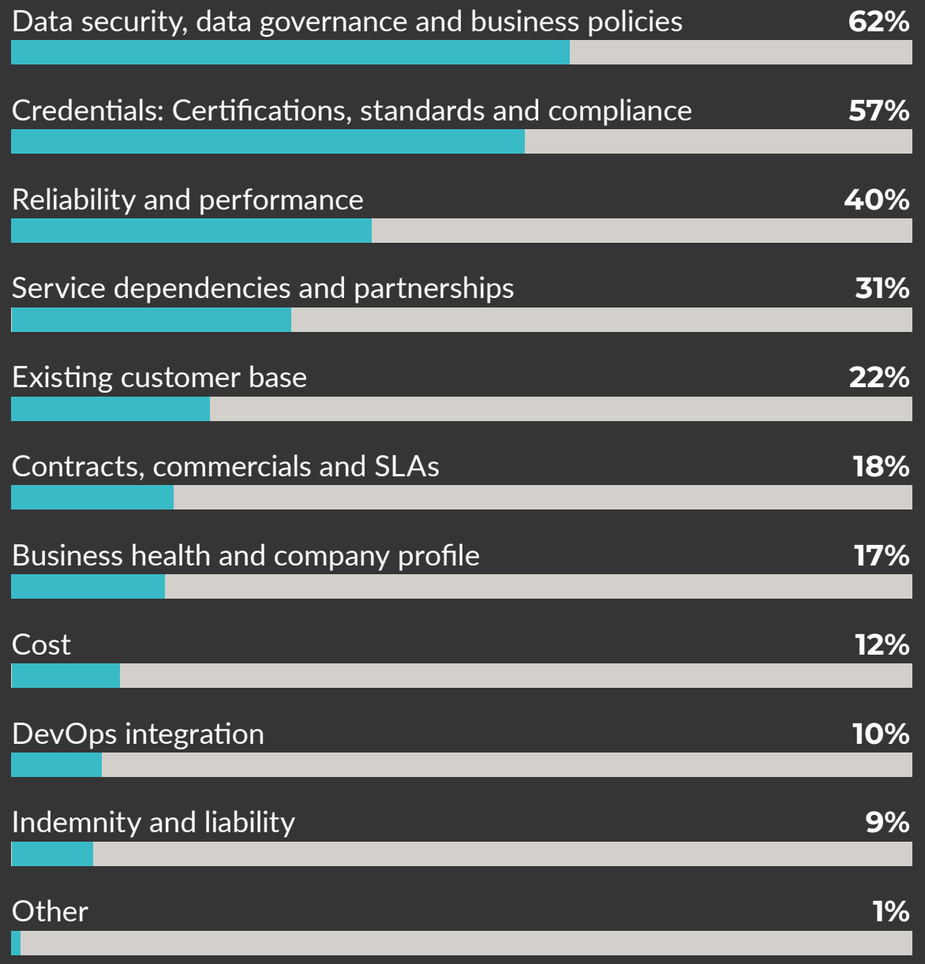
Base: Foundational, intermediate and advanced respondents (n=152).



Cost Takes a Backseat When Choosing Solutions

Healthcare organizations recognize the value of partnering with providers that have a proven history of consistent performance and cost ranks low, which is a significant departure from traditional procurement practices. This indicates a willingness to invest in premium security solutions to protect critical assets, as the financial consequences of data breaches far outweigh the investment.

What were/are your organization's most important criteria when selecting a cloud security and compliance solution?



Base: All respondents (n=181)
Multiple answers allowed.

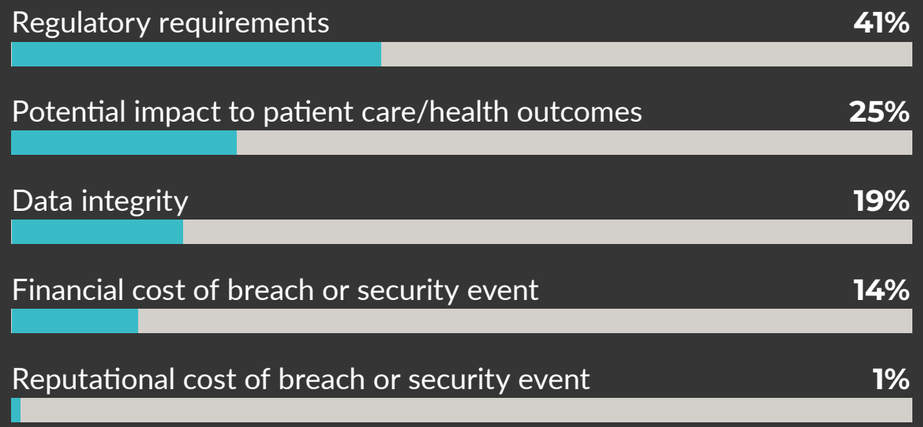
Compliance Outweighs Patient Safety

Adherence to regulations is undoubtedly essential, but only a quarter of respondents cite the potential impact on patient care and health outcomes as a key motivator. This suggests a missed opportunity to align cybersecurity with broader organizational goals that would enhance trust between healthcare providers and patients, strengthen the organization's reputation, and improve patient care.

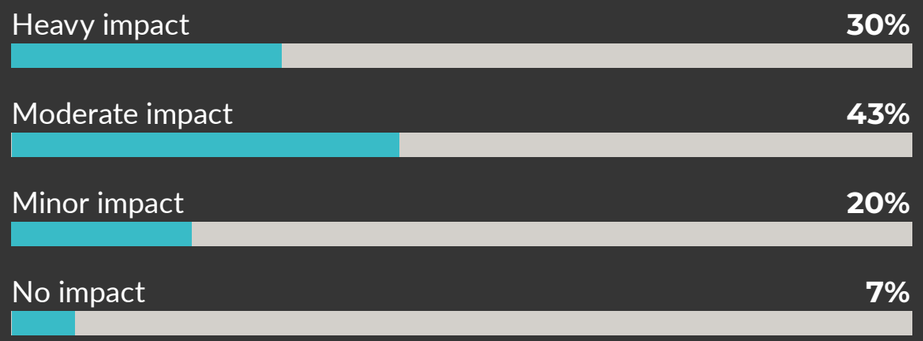
"These attacks and breaches of data can literally mean the difference between life and death for patients, significantly impact hospital operations, and — with the average hack costing millions to address — increase healthcare prices across the board."

— Senator Angus King (I-Me.), co-sponsor of the Healthcare Cybersecurity Act (July 11, 2024)

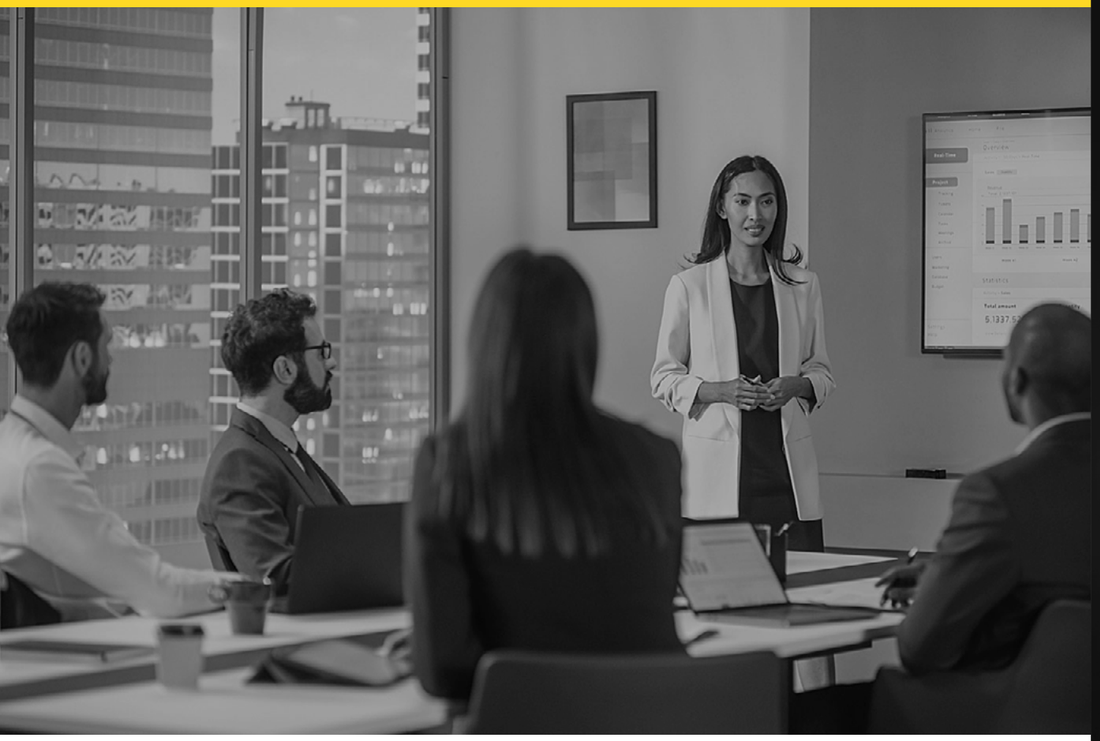
Which of the following would you consider to be the primary driver behind your organization's cybersecurity and compliance measures?



As regulatory requirements continue to evolve, how much have these changes impacted cybersecurity decisions?



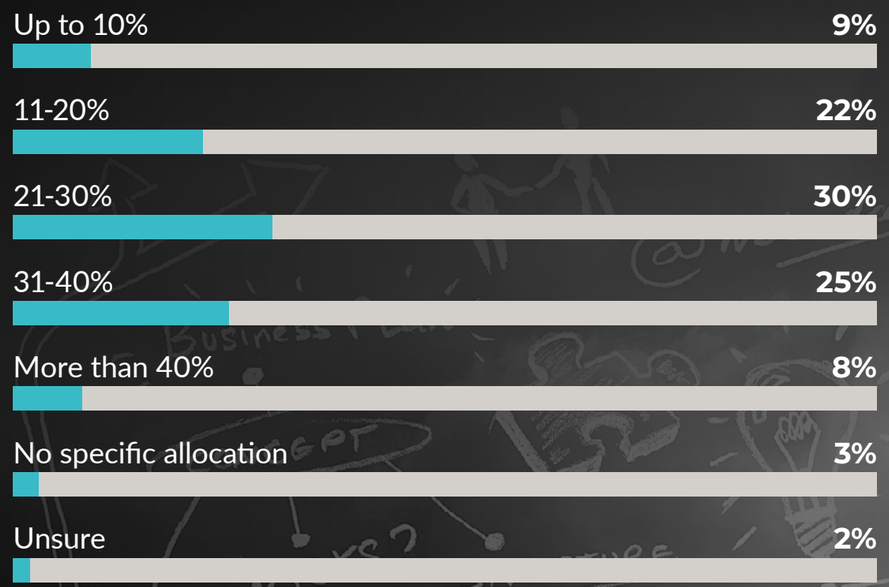
Base: All respondents (n=181)



Spending Is Increasing

There was a year-over-year increase in spending, with more than 50% of organizations using a significant part of their IT budgets for cybersecurity. These investments indicate heightened awareness of the risks and the imperative to comply with regulations. Additionally, while nearly a quarter of organizations' security budgets remained the same, 54% increased 10% to 20%.

What percentage of your organization's IT budget is allocated to cybersecurity and compliance?

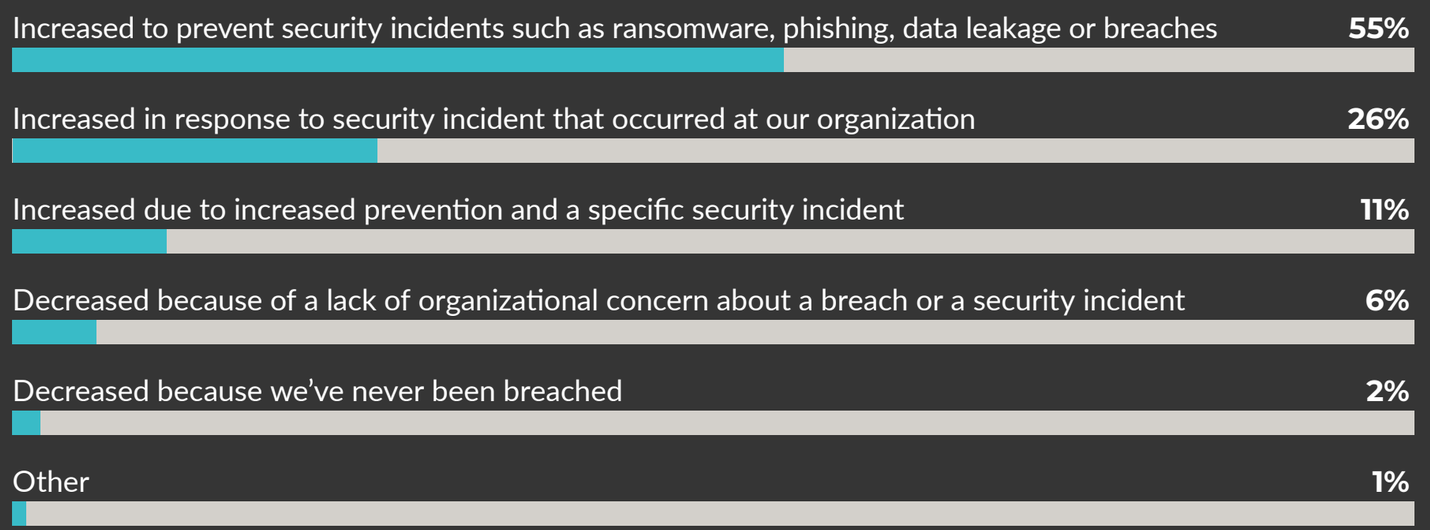


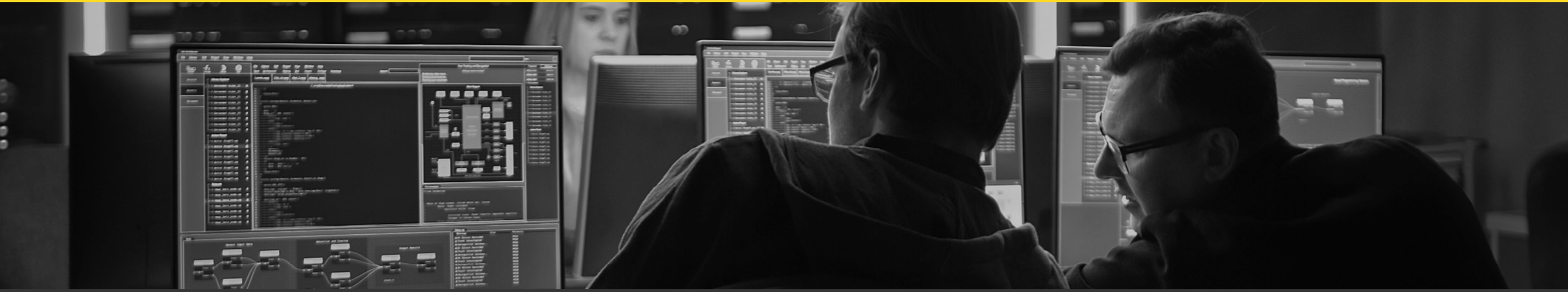
Base: All respondents (n=181)

Which of the following best describes the reason for your organization's decision to increase or decrease its cybersecurity budget?

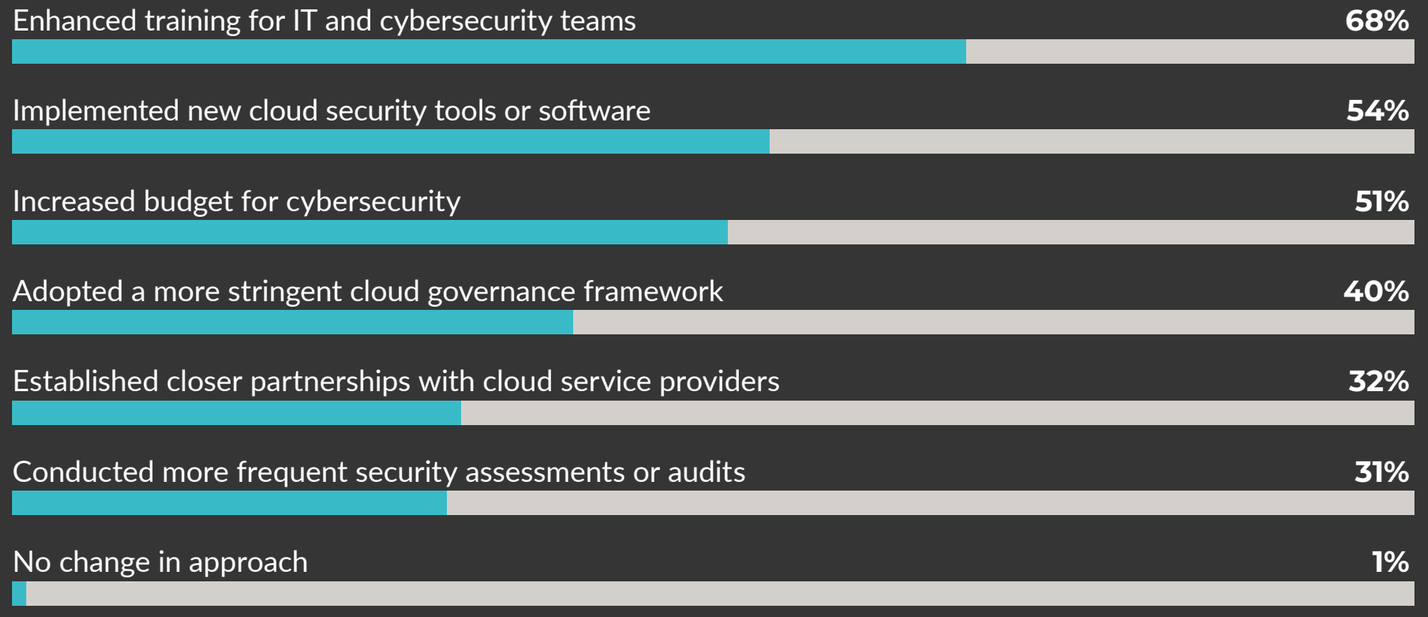
Base: Respondents with a budget increase or decrease (n=131).

92% of respondents said their cybersecurity budget is growing year over year.





Following the remediation of cloud misconfigurations, has your organization changed its approach to cloud security?



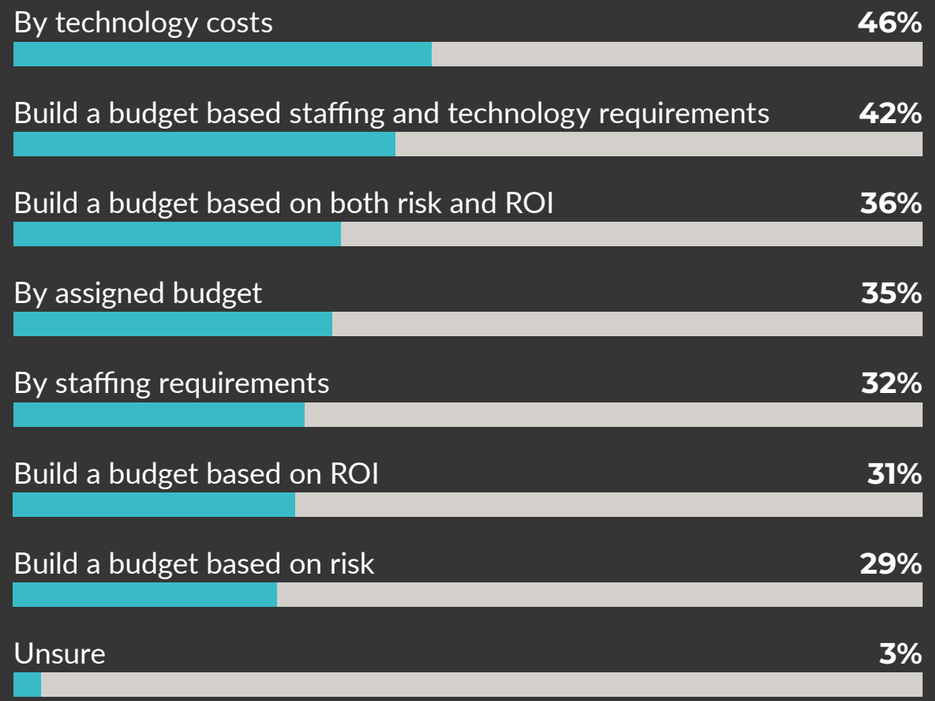
Base: Respondents with cloud misconfigurations (n=142).
Multiple answers allowed.

Staffing and Tech Drive Spending

Organizations realize the need to invest in sophisticated tools and skilled personnel. However, as misconfigurations and cyberattacks continue to increase year-over-year, in-house training may not be enough to fully protect sensitive data. Cultivating a deep knowledge of healthcare cybersecurity is time-consuming and costly, requiring a complex infrastructure, resources, and rapid deployment of advanced security measures 24/7 — cybersecurity threats don't take breaks.

Those who base cybersecurity spending on their organization's assigned budget may be overlooking the need for additional resources to adequately protect sensitive information.

How do you prioritize budget for your organization's compliance and cybersecurity efforts?



Base: All respondents (n=181).
Multiple answers allowed.

This report demonstrates the positive steps healthcare is taking to strengthen its cybersecurity defenses, but also stresses areas where IT teams could improve. While most leaders see themselves as increasingly sophisticated in their cloud adoption strategies, many don't feel as prepared as they should be for managing attacks, let alone preventing them.

Spending is way up, but nearly 80% of organizations experienced at least one cloud misconfiguration in the past year. Enhanced training is on the rise, but the persistence of misconfigurations suggests healthcare organizations need more help proactively addressing weak areas before problems surface.

Actionable Takeaways for Healthcare Leaders

- **SOLICIT INTERNAL FEEDBACK:** Conduct regular anonymous surveys, one-on-one meetings, and team-building exercises that encourage open dialogue to gain valuable insights about perceived capabilities, resources, and security posture.

- **PREPARE FOR EMERGING THREATS LIKE RANSOMWARE AND AI:** This involves continuous threat intelligence monitoring, robust risk assessments, and advanced security technologies. Foster strong partnerships with law enforcement, cybersecurity firms, and other providers to facilitate rapid response and recovery efforts.

- **REEVALUATE RESOURCES AND BUDGETS:** Quantify the effectiveness of existing security measures and compare costs to corresponding benefits. Consider reallocating funds to higher-impact initiatives or discontinuing underperforming tools. Leverage data analytics to correlate security spending with incident reduction and the full cost of cyber risks.

- **ASSESS THE FREQUENCY AND COST OF SECURITY AND COMPLIANCE INCIDENTS, INCLUDING MISCONFIGURATIONS:** Meticulous analysis of incident data allows you to identify patterns, root causes, and vulnerabilities, which is essential for prioritizing risk mitigation efforts, effective resource allocation, and measuring your ROI. Understanding the financial impact of security breaches — including remediation expenses, regulatory fines, and reputational damage — is also essential.

- **SEEK PARTNERS SPECIALIZED IN HEALTHCARE SECURITY AND COMPLIANCE:** Leverage their industry expertise, advanced tech, and tailored security programs. To streamline operations and reduce the risk of protection gaps, choose vendors with both security and compliance services, and a deep understanding of healthcare regulations (e.g., HIPAA, HITRUST).

CONCLUSION: Forging Ahead in Healthcare Security and Compliance

"The bad guys continue to innovate. We need to stay ahead of the curve and be vigilant and stay up to date…The promise of all this new technology brings new peril."
— Errol Weiss, Chief Security Officer at Health-ISAC (Healthcare Innovation)

Healthcare has taken great strides, but formidable challenges like budget constraints, overconfidence in cloud security, and data management complexities remain amidst a relentless onslaught of cyberattacks.

Addressing often-overlooked risks, such as cloud misconfigurations, aligning IT budgets with increasing cybersecurity costs — and choosing the right partners — are pivotal steps healthcare leaders can take. Adopting hybrid solutions and employee training is encouraging, but most healthcare organizations can't effectively manage cybersecurity and compliance without comprehensive, proactive strategies and specialized partnerships.

As the only healthcare-focused cloud expert with security, compliance, and cloud management services, ClearDATA is uniquely positioned to protect your data.

To learn more, visit cleardata.com.

We help healthcare organizations of all sizes meet regulatory requirements, stay resilient, grow, and scale amid evolving threats. We offer:

- Proactive CSPM software tuned to industry standards
- Comprehensive threat intelligence source
- Proactive threat hunting
- Cutting-edge MDR/XDR technologies
- Managed incident response services

Partnering with ClearDATA enables organizations to innovate at the speed of healthcare so they can focus on what matters most: patient health.

About the Survey

On May 10, 2024, Endeavor Business Intelligence emailed invitations to participate in an online survey to members of our *Healthcare Innovation* database. A panel of industry experts was also used to help with data collection. By May 20, 2024, Endeavor Business Intelligence had received 181 qualified responses to the survey.