

A False Sense of **Cybersecurity**

2022 State of Cloud Security
in Healthcare Providers

A REPORT FROM



CONTENTS

Introduction	4
Insight #1 Health providers may be overestimating their level of cloud maturity and cybersecurity preparedness	5
Insight #2 Cybersecurity is a top priority for midsize healthcare providers — but it's also the top barrier to cloud adoption	7
Insight #3 Larger provider organizations and those with more advanced cloud maturity primarily outsource their security and compliance solutions	9
Insight #4 The majority of healthcare providers have proactively increased their cybersecurity budgets in the last year, seeking to protect patient outcomes and remain compliant with evolving regulations	10
Conclusion	12

INTRODUCTION

One of the largest digital transformations in history is taking place across healthcare, reshaping the ways in which the industry engages with stakeholders and patients, treats both physical and behavioral wellness, and integrates real-time data and analytics into care models. By now, most providers and provider networks are migrating to the cloud and rapidly modernizing their technology infrastructures — with the ultimate goal of boosting efficiency, increasing accuracy, and providing not only a better patient experience, but better health outcomes.

Yet, at the same time, the industry continues to be plagued by cybersecurity and privacy events. After all, data is healthcare's most valuable and vulnerable asset, [worth as much as \\$1,000 per medical record](#) on the dark web. And as healthcare becomes increasingly digital, its attack surface expands as well — putting this treasure-trove of patient data at a far greater risk of compromise.

So how far along are providers on the path to modernization, and what are they doing to protect patient data? This report sheds light on the state of healthcare providers' cloud cybersecurity hygiene and investments, how the industry is evolving in the face of growing risks and increasing regulations, and where improvements can be made.

Ultimately, our research reveals an industry that is significantly unprepared and overconfident. While many providers believe their cloud infrastructure is well secured, the truth is they still have a long way to go to meet the minimum threshold for effective protection against an increasing attack surface.

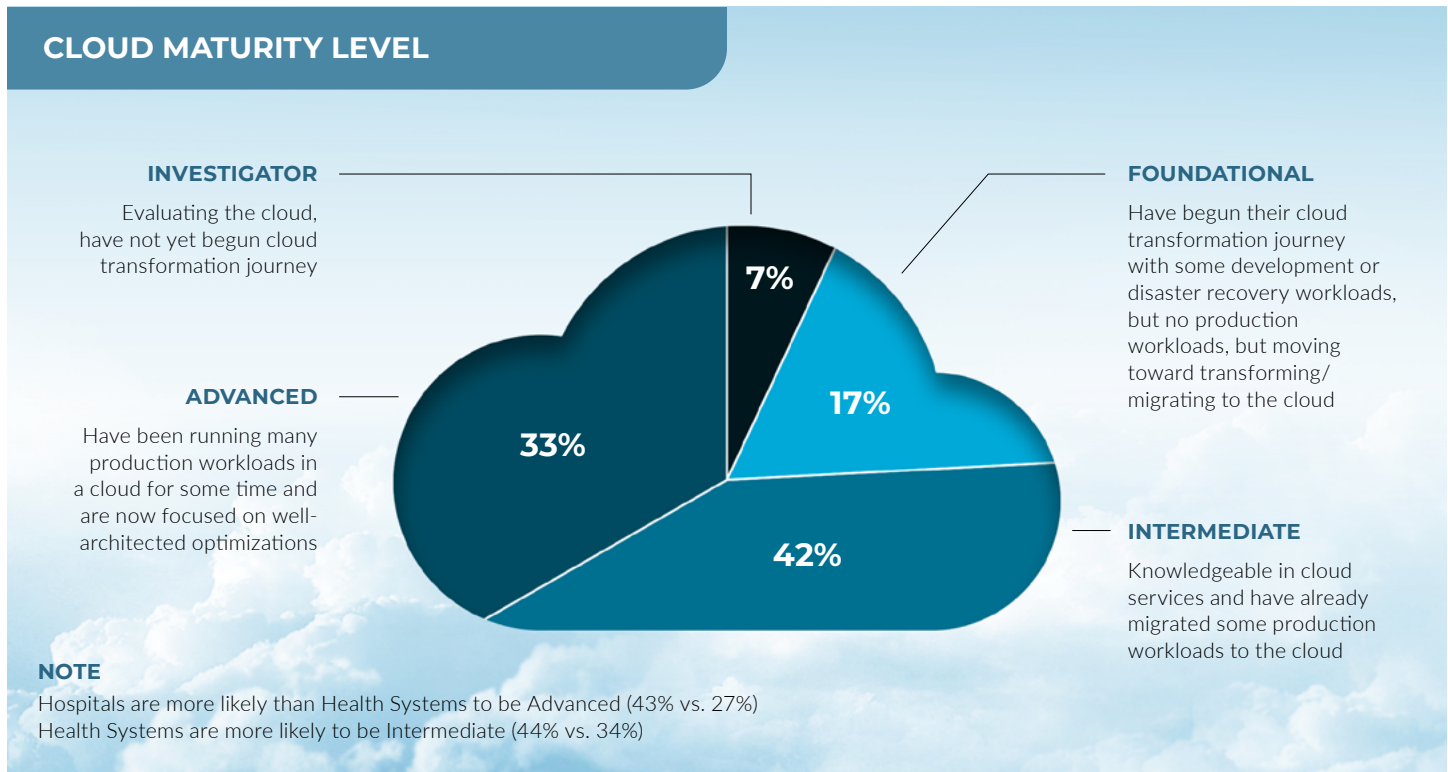
Four key insights emerged revealing how healthcare provider organizations are balancing cloud migration with cybersecurity preparedness to keep patient data safe:

- ✓ Health providers may be overestimating their level of cloud maturity and cybersecurity preparedness
- ✓ Cybersecurity is a top priority for midsize healthcare providers — but it's also the top barrier to cloud adoption
- ✓ Larger provider organizations and those with more advanced cloud maturity primarily outsource their security and compliance solutions
- ✓ The majority of healthcare providers have proactively increased their cybersecurity budgets in the last year, seeking to protect patient outcomes and remain compliant with evolving regulations

Research Methodology

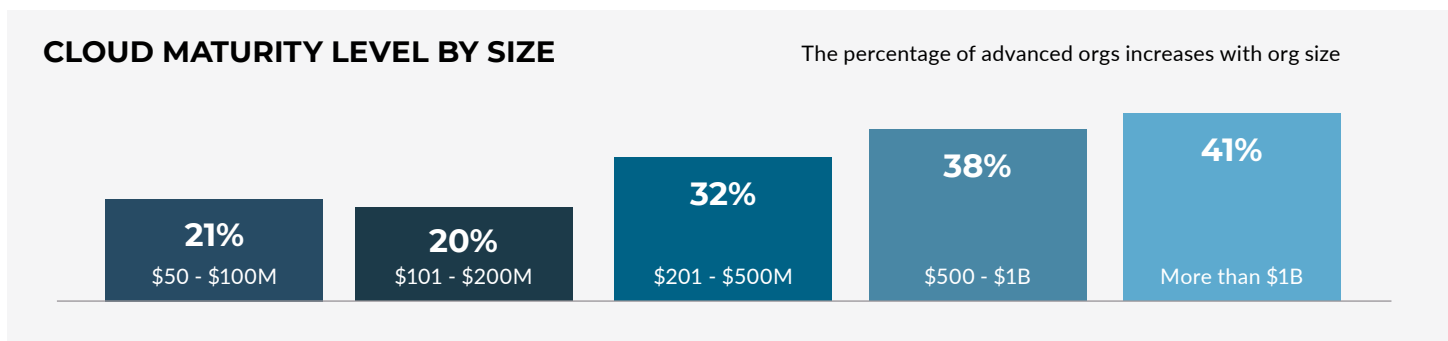
ClearDATA collected survey data from over 200 IT, security and compliance leaders at health organizations ranging from health systems, hospitals, healthcare providers, home healthcare organizations and ambulatory practices. The fieldwork was conducted May-June 2022 and surveyed participants on topics related to cloud maturity and infrastructure, cybersecurity priorities and preparedness, as well as cybersecurity budget. Participants' companies earn a minimum of \$50M in annual revenue.

Health providers may be overestimating their level of cloud maturity and cybersecurity preparedness



While healthcare has long been behind the curve when it comes to their technology and cybersecurity infrastructure (think: legacy systems), they are now making rapid progress in modernizing and catching up to other industries. In fact, the majority of our survey respondents say they are currently at an intermediate (42%) or advanced (33%) cloud maturity level. Only 17% report they are at an early, foundational level and 7% say they are currently investigating the cloud.

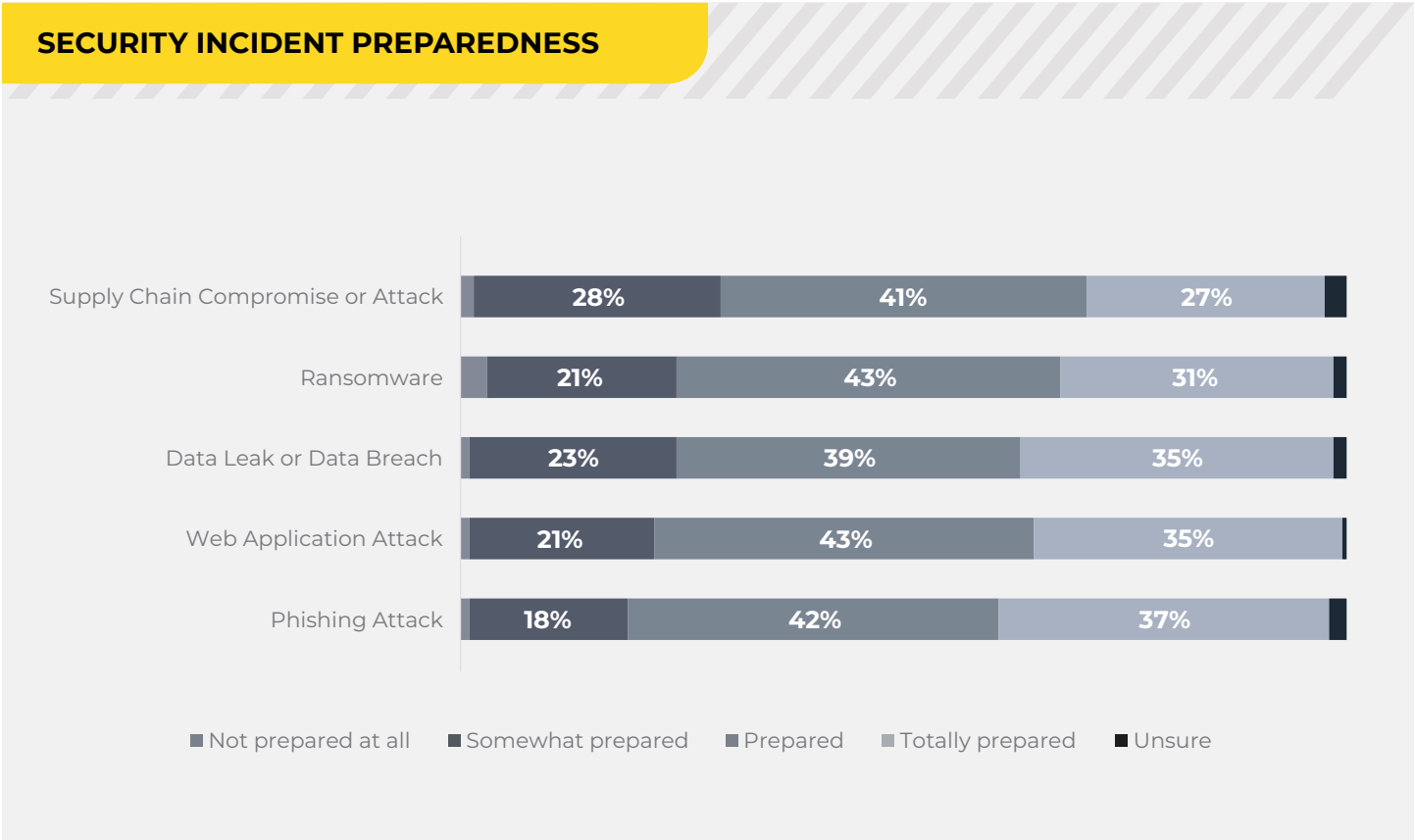
Notably, hospitals are more likely than health systems to be advanced (43% vs. 27%) and health systems are more likely to be intermediate (44% vs. 34%). We also see that the percentage of advanced organizations increases according to organization size, indicating that those with greater resources and larger teams have been able to progress further in their cloud journey and utilize the cloud for more workload types.



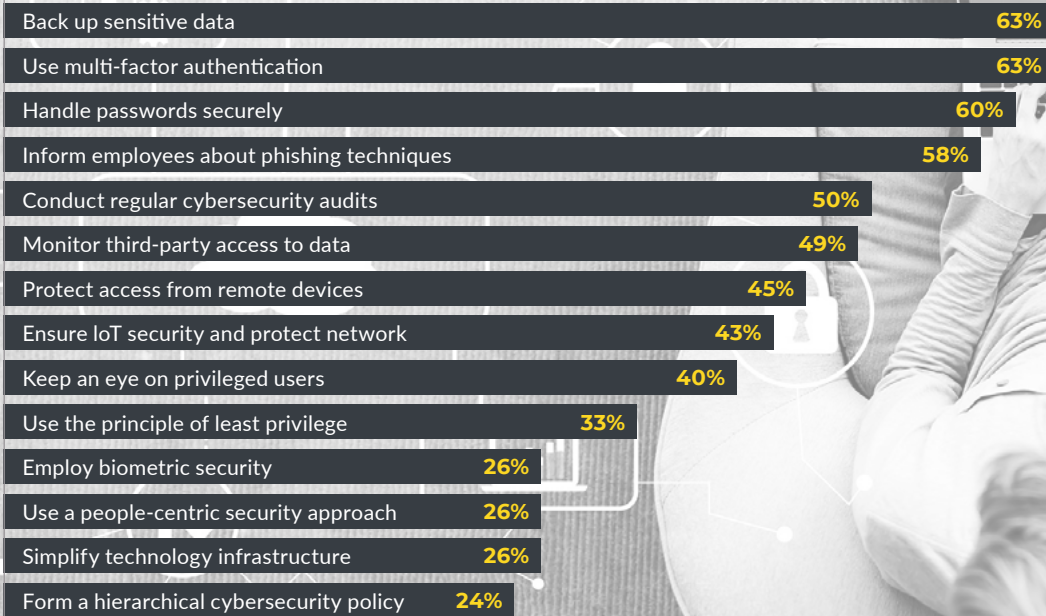
However, across the board, providers appear to be largely optimistic about how well their cloud infrastructure is secured. As many as 85% of respondents said they are confident in their cloud security and compliance program. But does this degree of confidence reflect the reality of cybersecurity preparedness? Maybe not. In fact, our research uncovered a significant disparity between how C-level executives and other leaders within an organization characterized their cloud maturity. Those at the c-level were much more likely than others to describe their cloud maturity level as advanced (64% vs. 20-28% of VPs, directors, and managers) indicating they may be overconfident in their assessment. Likely, being further away from the day-to-day realities may give them a false sense of security.



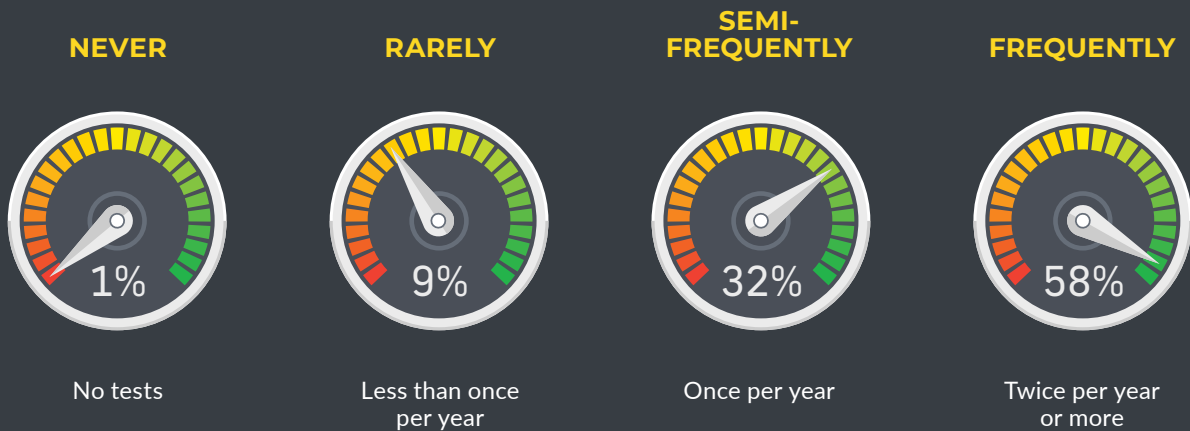
In addition, while most respondents report they are prepared or totally prepared for security incidents like supply chain attacks, ransomware, data breaches and phishing, many do not practice important risk reduction activities, including the most basic practices of backing up data, using multi-factor authentication and handling passwords securely. Even fewer providers have implemented more advanced tactics such as forming a hierarchical cybersecurity policy, simplifying technology infrastructure or ensuring IoT security. And while a little over half of providers (58%) frequently execute readiness tests or mock event/breach exercises, the rest do so only semi-frequently, rarely or never.



CYBERSECURITY RISK REDUCTION ACTIVITIES PRACTICED



FREQUENCY OF READINESS TESTS AND/OR MOCK EVENT/BREACH EXERCISES



QUESTIONS TO CONSIDER

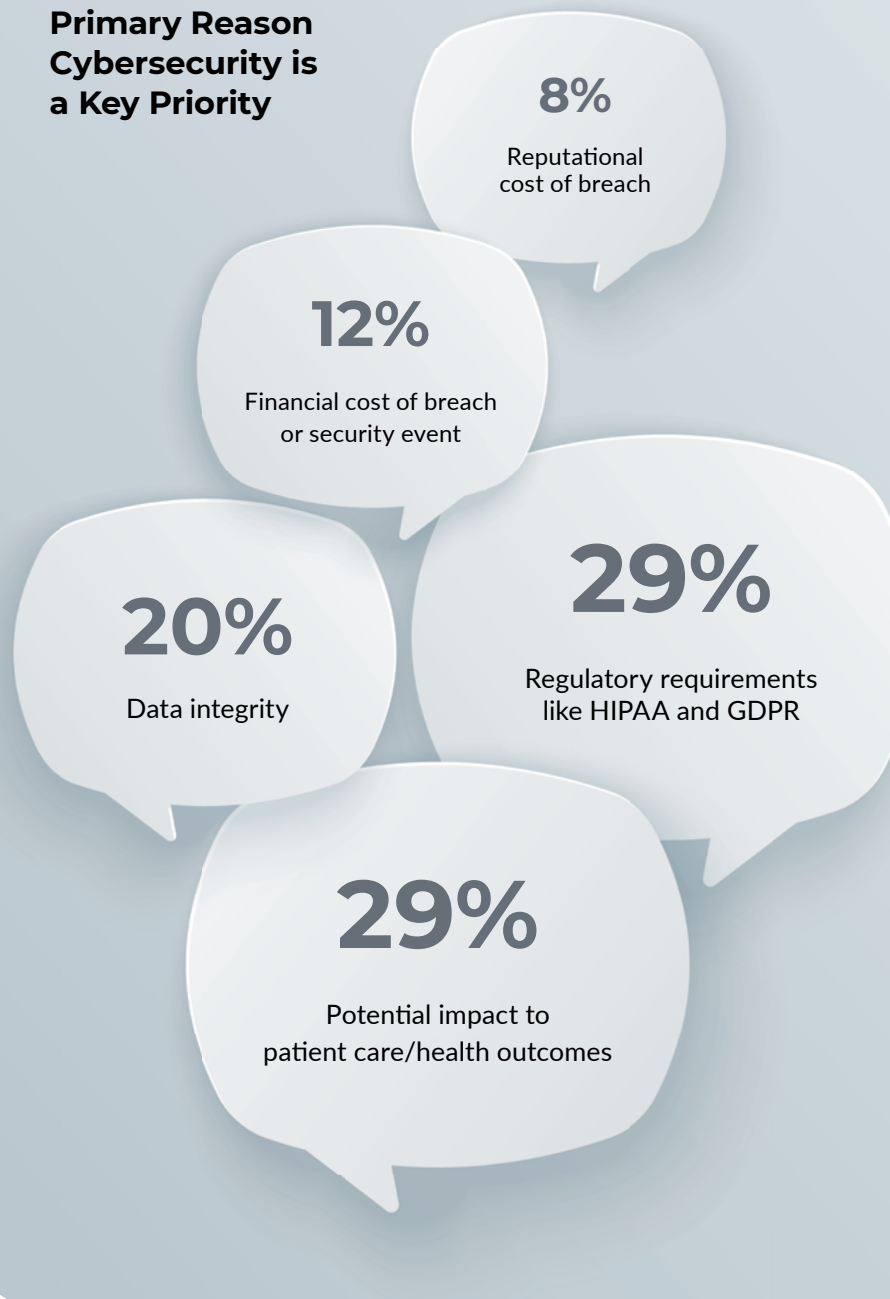
- ✓ What activities can your organization implement to boost cybersecurity preparedness?
- ✓ Is everyone in your organization on the same page about potential gaps and opportunities within your current cloud infrastructure?

Cybersecurity is a top priority for midsize healthcare providers — but it's also the top barrier to cloud adoption

In spite of modernization fears, [cloud adoption in healthcare is at an all-time high](#). And the stakes have never been greater. Healthcare providers understand that cybersecurity must remain a top priority to protect patient data in a digitally connected world. In fact, our survey respondents named their top reasons for prioritizing cybersecurity as the potential impact to patient care and health outcomes, along with regulatory requirements such as HIPAA and GDPR. Other key reasons included data integrity as well as the financial [cost of a breach](#).

Yet cybersecurity is also proving to be a major stumbling block preventing the industry from advancing toward digital transformation. For the majority of our survey respondents (56%), their biggest barrier to cloud adoption is cybersecurity. And the smaller a provider organization is, the greater the challenges seem to be: 63% of smaller providers (<\$500M) named cybersecurity as a top barrier, as compared to 50% of larger providers. These results underscore the complexity of navigating cloud migration, particularly, the accumulating cybersecurity implications that come with each new digital technology a provider adds — all of which smaller providers may be less equipped to manage on their own.

Primary Reason Cybersecurity is a Key Priority



TOP CLOUD ADOPTION BARRIERS OR CHALLENGES



6%	None
17%	Lack of In-House Expertise
32%	Compliance
32%	Data Management
35%	Budget
58%	Cybersecurity

Cybersecurity is a bigger issue for smaller orgs (<\$500M) than it is for larger orgs (63% vs. 50%)

QUESTIONS TO CONSIDER

- ✓ In what ways has your organization made cybersecurity a priority?
- ✓ What barriers are holding your organization back from cloud adoption?

INSIGHT #3

Larger provider organizations and those with more advanced cloud maturity primarily outsource their security and compliance solutions

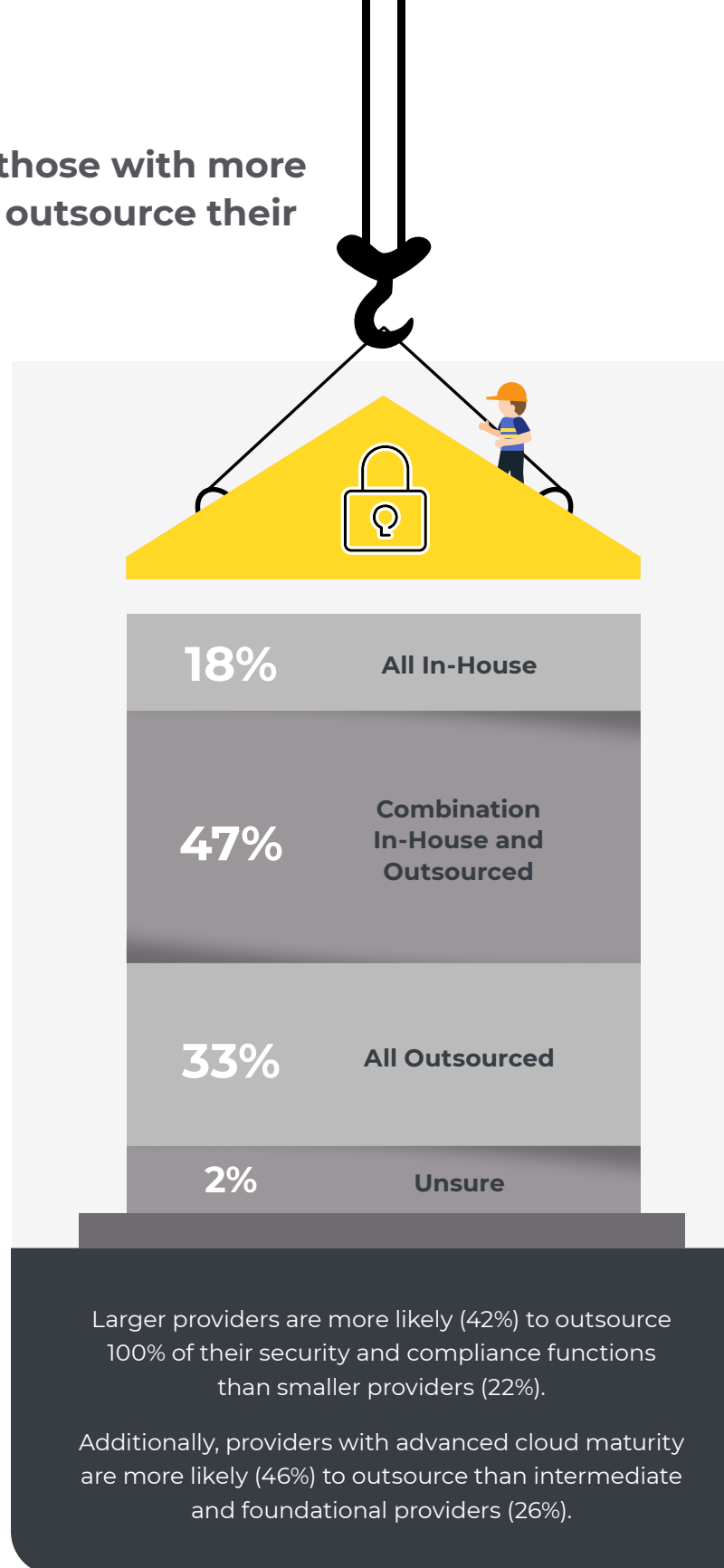
Keeping track of and managing the complete footprint of a patient's digital health data — how it is used, shared and stored — can be extraordinarily complex, and many providers lack the time and resources to do so, particularly given today's [cybersecurity talent shortage](#). That's why many providers choose to outsource. About one third (33%) of our survey respondents fully outsource management of compliance and security measures in the cloud, while 47% use a combination of outsourcing and in-house management.

Larger providers (>\$500M annual revenue) are more likely to outsource 100% of the management and tech solutions for security and compliance (42% vs. 22% for smaller providers), indicating that, even with greater internal resources, these organizations still recognize the value of partnering with third-party cloud experts.

In addition, providers with advanced cloud maturity are also more likely to outsource (46% vs. 26% for intermediate and foundational). This makes sense, given that providers who are further along in their cloud journey are likely to require external help to manage the increasing complexity or, perhaps, have achieved their more advanced state due to outsourcing to cloud experts earlier on.

QUESTIONS TO CONSIDER

- ✓ How could your organization benefit from outsourcing its security and compliance solution?
- ✓ If using a combination of outsourcing and in-house management, how can you best integrate your internal and external teams?



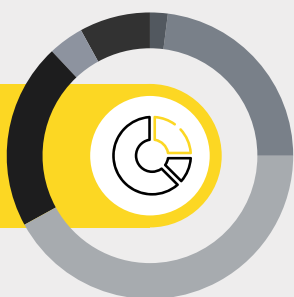
The majority of healthcare providers have proactively increased their cybersecurity budgets in the last year, seeking to protect patient outcomes and remain compliant with evolving regulations

Unsurprisingly, as cyber risks and compliance regulations rise, so do security budgets. However, it may surprise you just how many healthcare providers increased their budgets proactively, rather than waiting for a security incident to arise.

According to our survey respondents, only 26% of cybersecurity budgets remained the same compared to the previous year.

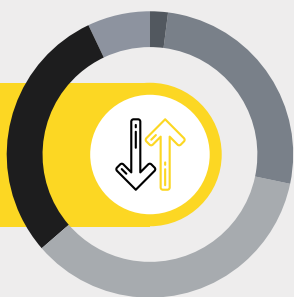
Meanwhile, 71% of budgets grew — with 35% increasing less than 10%, 29% increasing by 11-24% and 7% increasing more than 25%. And in as many as 81% of cases, the decision to increase budget was made proactively to prevent potential security incidents.

CYBERSECURITY BUDGET



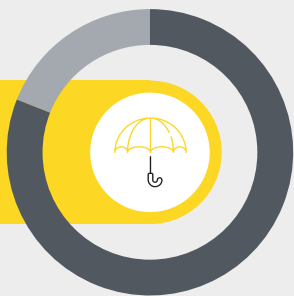
PERCENTAGE OF IT BUDGET

2%	Up to 5%
23%	6-10%
42%	11-15%
21%	More than 15%
4%	No specific allocation
8%	Unsure



CHANGE COMPARED TO PREVIOUS YEAR

2%	Decreased
23%	Remained the same
42%	Increased less than 10%
21%	Increased by 11-24%
7%	Increased by more than 25%



DECISION TO INCREASE BUDGET

81%	PROACTIVE	Prevention of security incidents such as ransomware, phishing, data leak, or breach
19%	REACTIVE	Organization experienced a security incident and increased cybersecurity budgets to mitigate

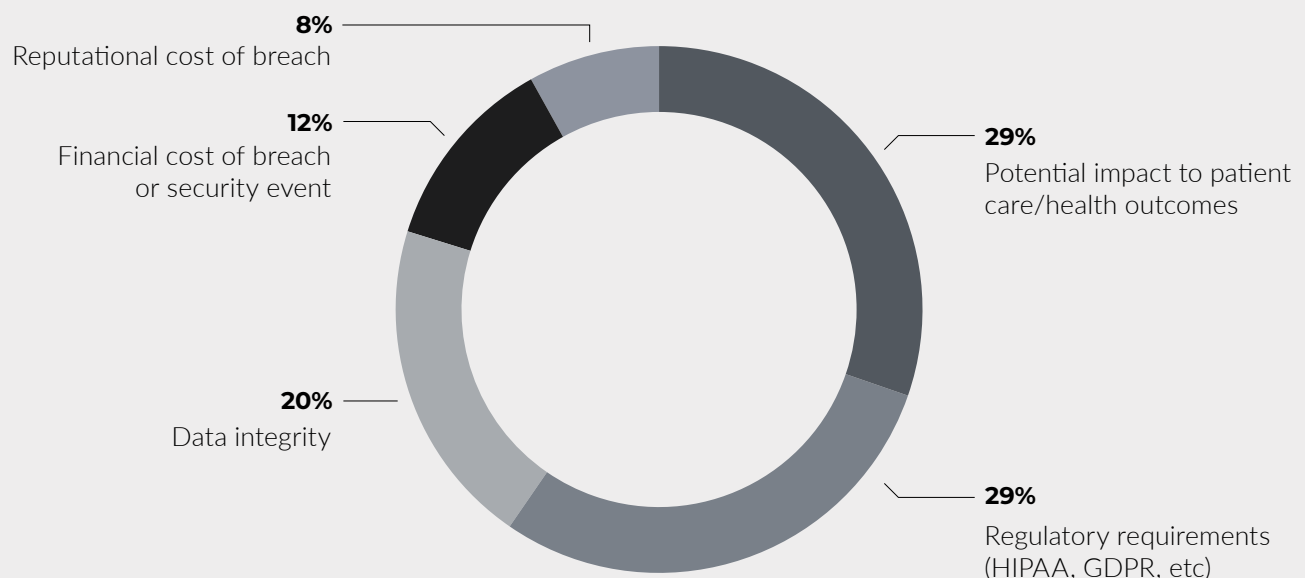
TOP PROVIDER CONCERNS

What are healthcare providers most concerned about preventing? Respondents named their top three security concerns as: data leaks or breaches, ransomware and phishing. All of these incidents, of course, carry the potential to negatively impact patient health — which may well be the worst fear of every healthcare provider, and a primary reason behind growing cybersecurity investments.

MOST CONCERNING SECURITY INCIDENT AMONG RESPONDENTS

- 41%** Data leak or breach
- 29%** Ransomware
- 15%** Phishing attack
- 9%** Supply chain attack
- 5%** Web application attack

PRIMARY REASON CYBERSECURITY IS A KEY PRIORITY



IMPACT OF REGULATORY REQUIREMENTS ON CYBERSECURITY DECISIONS

Healthcare providers are also highly concerned with meeting evolving regulatory requirements, which have had a significant impact on cybersecurity decisions, including those pertaining to budget. 43% of our survey respondents said regulatory requirements have a heavy impact and 54% said they have a moderate impact on their cybersecurity decision making. As regulations continue to increase going forward, we can expect to see even greater investments in cybersecurity as providers strive to remain compliant in safeguarding personal patient data.

QUESTIONS TO CONSIDER

- ✓ Has your organization taken a reactive or proactive approach to cybersecurity budgeting?
- ✓ What factors have the greatest impact on your cybersecurity budget? What is your “why” behind investing in cybersecurity?


CONCLUSION

While healthcare providers across the board are making important strides toward cloud maturity and security, they must also understand and address the gaps in their technology infrastructure and cybersecurity practices to ensure their success in a rapidly changing industry.

Indeed, some healthcare leaders may be overconfident in their organization’s current cloud maturity level, as well as how prepared they are in the event of a serious security incident. (To say nothing of the evolving regulations.) For many providers, there is still a significant opportunity to strengthen their cybersecurity posture — from the basics of multi-factor authentication and security training for employees, to implementing more advanced tactics like streamlining and modernizing their technology infrastructure.

Not only will these practices help providers migrate to the cloud faster and more seamlessly, ushering in a new, modern era of healthcare delivery, there’s simply no better way to protect vulnerable health data and improve patient care. But, the truth is, most providers can’t do it on their own.

That’s why, at ClearDATA, this is our sole focus. As a cloud catalyst and healthcare protector, we are dedicated to securing data and putting it in the right hands, exactly when it is



43%	Heavy Impact
54%	Moderate Impact
1%	No Impact
2%	Unsure

needed. Data managed by ClearDATA is timelier and easier to access than data siloed and disconnected, an advantage which ultimately leads to better healthcare.

From fledgling start-ups to large enterprises, healthcare providers turn to ClearDATA for guidance at every stage of their cloud journeys, whether planning a new application, balancing a complex multi-cloud strategy, or scaling a mature cloud operation. ClearDATA’s healthcare-specific managed services offer a trifecta of benefits: protecting healthcare data in the cloud while minimizing false positives and decreasing response times; automatically preventing, detecting and remediating compliance drift and PHI security gaps; and integrated privacy and security controls — all so clients can innovate at the speed of healthcare and focus on what matters most: patient health.

ABOUT CLEARDATA

ClearDATA is healthcare’s largest managed cloud and defense provider, enabled by our powerful CyberHealth™ SaaS platform. Its solutions operationalize compliance, privacy and security for the healthcare ecosystem in the public clouds. To learn more about how ClearDATA delivers a secure and scalable healthcare cloud for market-leading organizations, visit cleardata.com.