VERITAS

2023 HEALTHCARE REPORT

DATA RISK MANAGEMENT

The State of the Market—Cyber to Compliance

Research conducted by: VansonBourne

INTRODUCTION

The ability to manage risk is a foundation of a successful organization. Those that do it well can navigate challenges, while their competitors struggle. Recent years have seen a succession of heightened risks with contributing factors including a pandemic, geopolitical tensions, and economic turmoil. As a result, organizations are facing risks from every conceivable angle. Those that manage them best are the most likely to succeed.

Individual industries approach the topic of risk management differently, as do individual organizations and employee groups. This report is a subset of 202 business executives and IT practitioners in the healthcare sector from a global research survey with 1,600 respondents.

This report looks to answer the following questions:

What are the greatest risks facing healthcare organizations today? How does this compare to other industries?

When it comes to data security, how have healthcare organizations adapted to threats in recent years?

Do healthcare organizations and their employees believe themselves to be at risk? How does this translate into action?

KEY FINDINGS

Data security is the top concern for healthcare organizations.

- Risks to data security (**43%**) ranked highest, followed by economic uncertainty (**39%**), emerging technologies like AI (**32%**), and talent shortage (**32%**).
- **85%** of healthcare respondents report actual damage, such as financial and reputational damage, from risks. This is slightly less than those who say the same globally (87%).

Organizations are increasing data protection budgets and staffing in response to risk.

- Despite being one of the industries most at risk for cyberattacks, healthcare organizations have increased their data protection budgets only **20% to 25%** on average—much less than the global average.
- Staffing increases for data protection and data security teams are also substantially lower at an average of **15** employees each.

The healthcare sector is under attack.

- **76%** of healthcare respondents report they have experienced a successful ransomware attack in the past two years. This figure is substantially higher than the global average of 65%. Moreover, healthcare is the sector third most at risk for experiencing an attack.
- **65%** of healthcare organizations have experienced data loss in the last two years from events other than ransomware attacks, also higher than the global average (48%).
- Average data loss is **11% to 12%** across IT environments measured in the same timeframe.

Risk levels have increased for most categories in the healthcare sector.

- Respondents are more likely to report that risk levels have increased rather than decreased for all types of risks measured. Data security (**61%**) and talent shortage (**60%**) had the most respondents indicating increased risk levels.
- **62%** of healthcare organizations believe their organization is currently "at risk," a figure substantially higher than the global average of 52%.

Healthcare organizations report data security and economic uncertainty as their biggest concerns.

Managing risk is necessary for every organization. And with risks increasing in sophistication, adaptation is essential for survival. In fact, the threats in healthcare are higher than in many industries, with 76% reporting they have experienced a successful attack in the last two years.

It's important that leaders in healthcare organizations understand the risks they face today and those that are increasing within their sector. With clarity about the threat landscape, they can take appropriate measures to mitigate any potential risks.

The Greatest Risks to Healthcare Organizations Today

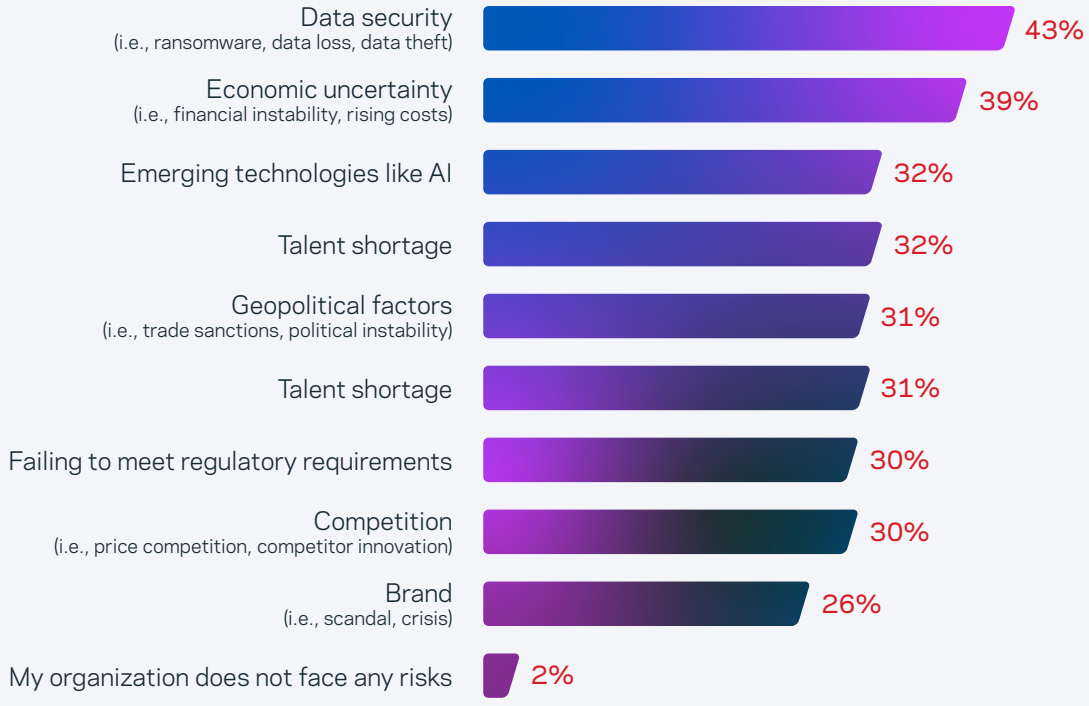


Figure 1. Which of the following are the greatest risks to your organization today? Combination of responses ranked first, second, and third. [202] Data shown only from organizations in the healthcare sector; not all answer options shown.

85% of respondents say risks have resulted in actual damage to their organization.

47% of healthcare organizations experience damage from data security.

There will be a global shortfall of **10 million** healthcare workers by 2030.

Healthcare organizations report their top risks as data security (43%), economic uncertainty (39%), emerging technologies like AI (32%), and talent shortages (32%) (Figure 1). In general, these align with the general trend. While the higher rank of talent shortages is unique to healthcare, it's unsurprising. According to the World Health Organization, there will be a global shortfall of 10 million healthcare workers by 2030. Additionally, the shortage will affect low and lower-middle income countries more heavily due to the lack of budgetary capacity within the public sector to afford healthcare workers.

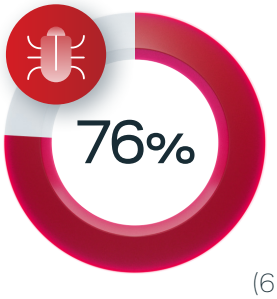
Data risk and data security are not new topics for healthcare organizations. In fact, according to Verizon's 2023 Data Breach Investigations Report, of 5,199 confirmed data breaches in 2023, healthcare experienced 477, behind only public sector and financial services organizations.

Data breaches have a variety of consequences ranging from reputational damage and downtime to financial costs. IBM states the average cost of a data breach was $4.45 million USD in 2023—rising to $10.9 million USD in the healthcare industry. With the sector already experiencing economic hardship, improving data security could have economic advantages.

In the healthcare sector, 85% of respondents report having experienced actual damage from risk. The most likely source? Data security. More healthcare organizations experience damage from data security than the all-sector average (47% and 40% respectively).

Damage is inevitable, but organizations need to make consistent efforts to ensure they're prepared for any potential data security risks. The consequences of a successful attack have the potential to be astronomical for healthcare organizations.

Many healthcare organizations have experienced successful cyberattacks and data loss.



Of the organizations surveyed, 76% report having experienced a successful ransomware attack in the last two years in which attackers gained access to the targeted system (Figure 2). This is higher than the all-sector average (65%), and the third highest behind only media, leisure, and entertainment (81%) and energy, oil/gas, and utilities (78%).

This higher exposure to attacks is only part of the threat environment. In fact, 65% of healthcare organizations state they have experienced data loss from a source other than ransomware. Only the media, leisure, and entertainment sector (70%) has experienced higher loss. It's clear the healthcare sector is vulnerable to risk. How organizations address the challenges will be essential to ensure long-term success.

Although only 62% of healthcare respondents report feeling at risk, 76% have experienced a successful ransomware attack in the last two years. What's more, when compared to other industries, healthcare is experiencing a higher rate of successful attacks. Organizations need to better equip themselves to prepare against cyberattacks to reduce risk. Overall, 29% of healthcare organizations report that they don't expect their organization to survive another 12 months, which is substantially higher than the 15% all-sector average and the highest compared to other industries surveyed.

Despite the higher rate of successful ransomware attacks, healthcare organizations have managed to limit their impact, as shown by lower-than-average data loss across surveyed environments. Cyberattacks will continue to evolve which means risk awareness and tailored mitigation strategies will be fundamental to ensure long-term survival.

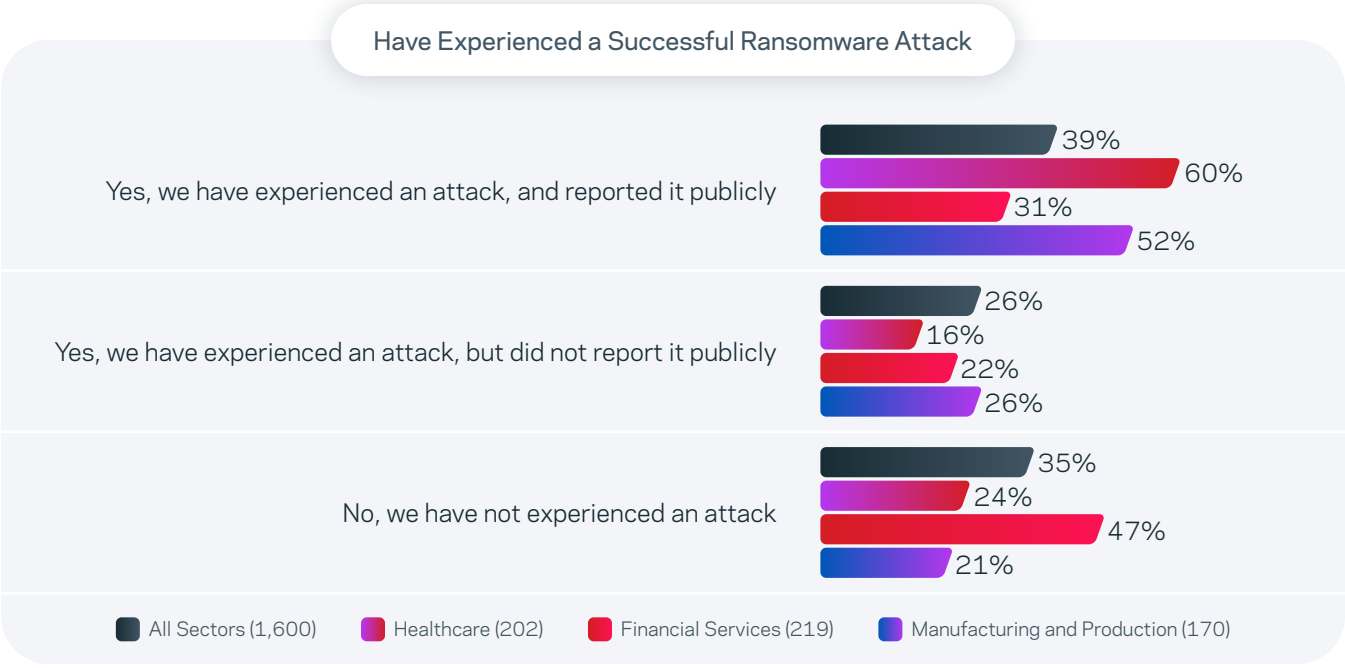


Figure 2. Has your organization experienced a successful ransomware attack in the last two years? [Base sizes in chart] Data split by sector, showing data for healthcare, financial services, and manufacturing and production; not all answer options are shown.

The healthcare sector is increasing budgets and staffing in response to the growing risk environment.

Healthcare organizations have increased their data protection budgets to better protect data security by an average of 20% to 25% over the past 12 months (Figure 3). Given that data security risks have caused the most damage in the sector, it's surprising that organizations aren't increasing their budgets as much as other sectors. This may be a result of the additional risks from economic uncertainty.

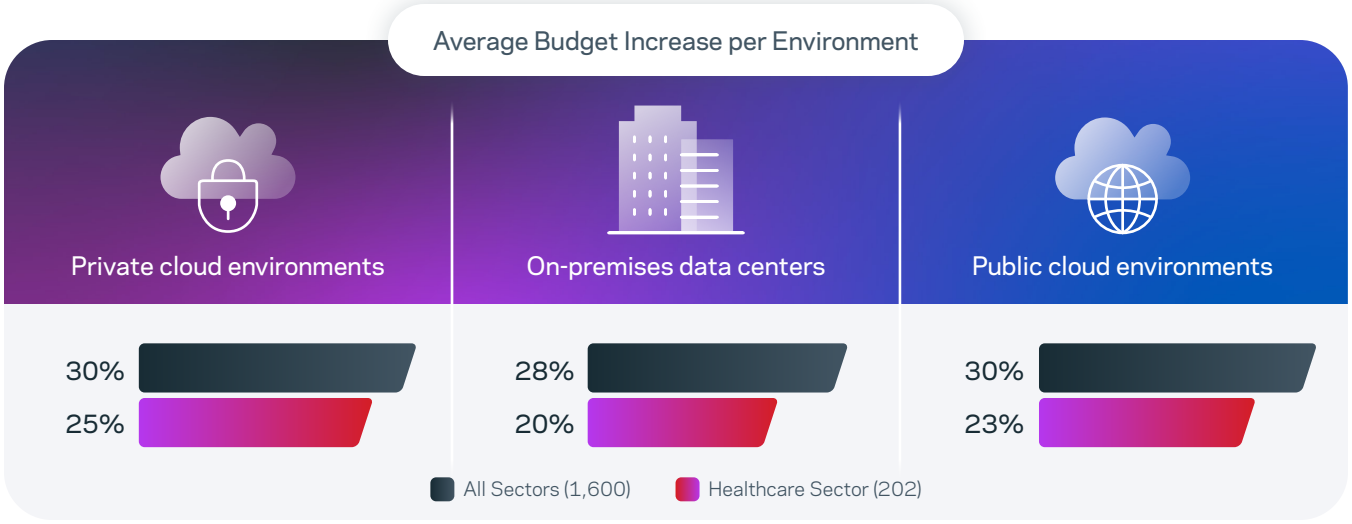


Figure 3. Approximately, how has your organization's budget for data protection changed in the last 12 months over the following environments? [Base shown in chart] Chart shows only the average percentage increase per environment; showing data from all sectors and the healthcare sector.

15 People

Average staffing increase of data protection and data security teams.

In addition to the budget increases across surveyed environments, healthcare organizations have marginally increased their data protection and data security teams by an average of 14 and 16 people, respectively. This is substantially lower than the all-sector average of 21 and 22 people per team. However, any progress in increasing team sizes is a step in the right direction to improve risk mitigation.

Healthcare organizations face a variety of growing risks.

Risks are constantly evolving and changing. What may be a priority one year won't necessarily be the same the next. The healthcare sector knows this well, with at least 40% of organizations reporting an increase in all identified risk factors (Figure 4). Risks from data security continued to rise in the last 12 months, as reported by 61% of healthcare organizations. This is to be expected given it's currently causing the most damage. This finding also aligns to the widely publicized vulnerability of the healthcare sector.

Only two percentage points separate the top three on the list, with talent shortage (60%) and risks from emerging technologies like AI (59%) just behind data security.

Moreover, the respondent perception of increase across these three factors exceeds the all-sector averages (54%, 51%, and 54%, respectively). The healthcare sector will have to focus on diversifying mitigation strategies across different risks.

Despite many organizations reporting increased risk across multiple factors in the last 12 months, it seems many still underestimate the current threat. While 62% currently report they feel at risk in general, it's only a portion of those that acknowledge experiencing specific risks the last two years (98%). The perception of current risk is also lower than those reporting they have experienced damage from risks in the last two years (85%).

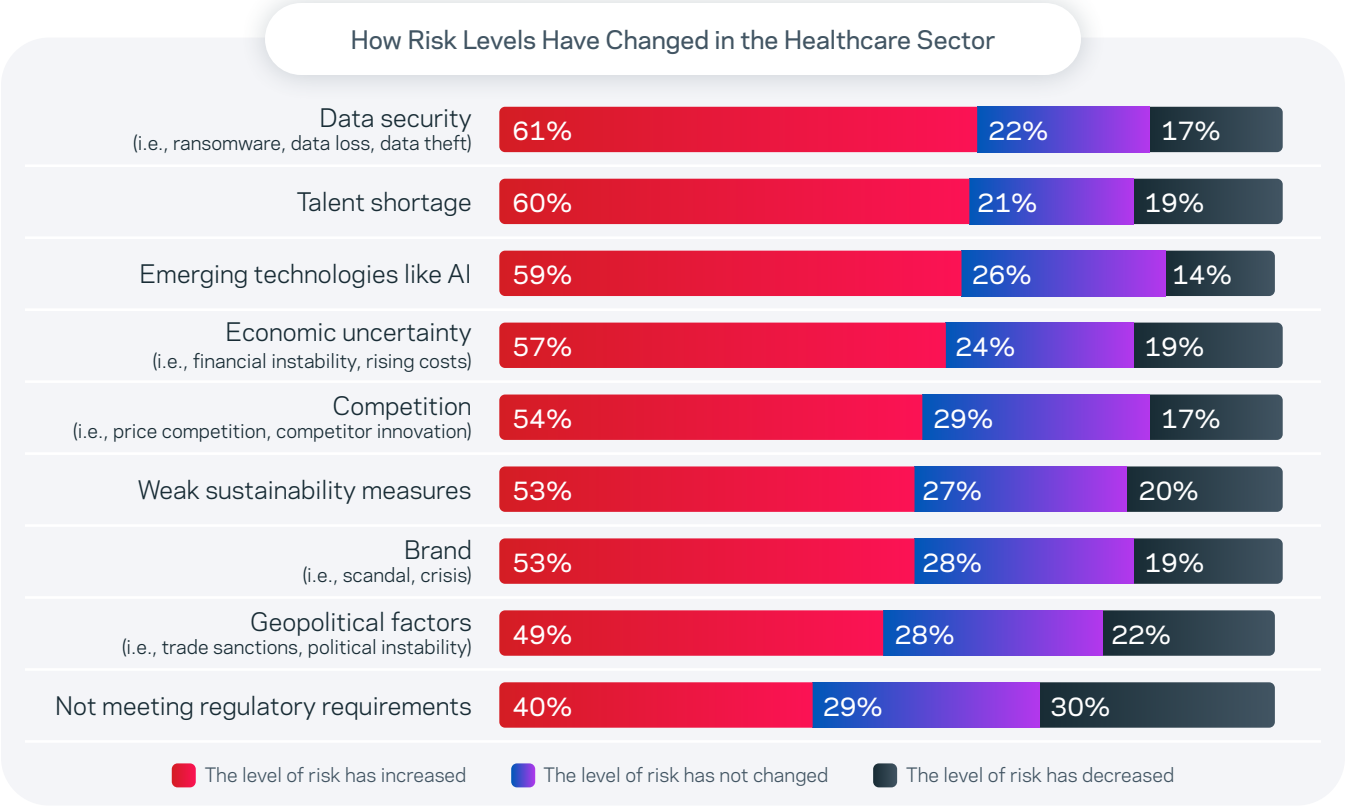


Figure 4. How has the level of risk to your organization over the following categories changed over the past 12 months? [198] Question shown only to those who state they experience risks today. Chart shows data only from the healthcare sector and does not include all answer options.

CONCLUSION

Risks are constantly evolving across all organizations, regardless of industry. The healthcare sector is under attack, facing more successful ransomware attacks than other sectors and with more respondents identifying increased risk levels across risk types. Healthcare organizations need to prepare to manage these different risks as they evolve. Those that fail will find it hard to survive in the turbulent risk environment.

There is good news, however. Healthcare organizations have made positive strides in their data protection strategies as seen by lower data loss from incidents other than ransomware. Additionally, many are increasing investments in data protection, security, and staffing in the next 12 months. Both are a step in the right direction as they prepare to handle the risks that face them.

Research Scope and Methodology

Veritas Technologies commissioned independent market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 1,600 business executives and IT practitioners were interviewed during August and September 2023, with representation from the following regions and individual markets (number of interviews in brackets):

- **Americas (300):** US (200), Brazil (100)
- **EMEA (500):** UK (100), France (100), DACH (100), Nordic (100), UAE (100)
- **APAC (800):** China (200), South Korea (100), Singapore (100), India (200), Japan (100), Australia (100)

All respondents had to be from organizations with more than 1,000 employees and represent a range of private and public sectors including: Biopharma; Business and Professional Services; Construction and Property; Consumer Services; Energy, Oil/Gas, and Utilities; Financial Services; Healthcare; Healthcare Products and Technology; IT, Technology, and Telecoms; Manufacturing and Production; Media, Leisure, and Entertainment; Retail, Distribution, and Transport; and Other Commercial Sectors. All respondents had to at least influence technology purchasing within their organizations.

Vanson Bourne conducted interviews using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

This executive summary is based on the data from the healthcare sector, with comparisons made to the data from other sectors where applicable.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

VansonBourne

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value.

VERITAS

V2046 2/24