

A MATTER OF LIFE AND DEATH

HEALTHCARE CYBER RECOVERY READINESS REPORT

2024



In partnership with **GIGAOM**

CONTENTS

Introduction	3
A Breach Can Teach	4
Cyber Challenges to Overcome	6
Testing Is Vital to Cyber Resilience and Readiness	8
Markers of Cyber Maturity	9
Cyber-Ready Organizations Recover Faster	11
A Prescription for Preparedness	12
Demographics	13

INTRODUCTION

Preparing for and responding to a breach are critical factors in cyber resilience at healthcare organizations.

Unfortunately, breaches are far too common, affecting companies of all sizes across all industries.

In the first 3 quarters of 2024 alone, **U.S. healthcare organizations have been hit by cyberattacks**



386 times¹

And when an incident disrupts hospital operations and delays patient care, it can quite literally be a matter of life and death.

Like any dramatic experience, the experience of fighting through a breach reshapes how an organization behaves and prioritizes its actions. These were among the findings in our inaugural [Cyber Recovery Readiness Report](#), a joint effort of Commvault and GigaOm. We've taken a closer look at the findings and how they apply across the healthcare industry, which must contend with a wide set of sensitive data to protect, changing regulations, reliance on third parties, and aging infrastructure.

We surveyed 1,000 cyber security and IT leaders from countries around the world to better understand the global state of cyber recovery readiness and to get a clear understanding of how organizations remain resilient through the chaos and damage of breaches. **Sixty-three of the leaders worked in healthcare**, with 43 employed at large healthcare organizations with more than 5,000 employees. See more details about our methodology and respondents on [Page 13](#).

Our survey confirmed the prevalence of breaches, with 83% of our respondents reporting a material security breach: over 50% of these within the past year and more than 75% in the last 18 months. Given that the average cost of a breach in 2024 is \$10 million for healthcare organizations (making it the most expensive recovery costs of any industry)², remaining resilient by protecting against them and recovering quickly is paramount.

A BREACH CAN TEACH

The experience of a breach has significant impact on how an organization approaches resilience.

One significant finding across the data set is that there are many lessons to be learned from being breached. Organizations gain experience that changes their outlook, prioritization, and often, their maturity.

As an example, **healthcare organizations** that experienced a breach are nearly **3.5 times more likely** to rank understanding data risk profile, data classifications, and relative level of risk as a top priority for their cyber recovery strategy, compared to organizations that have not been breached (Figure 1).

Figure 1



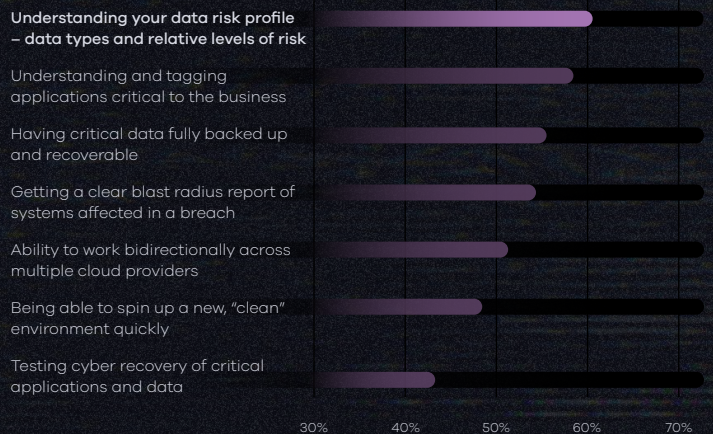
In response to security incidents, what priorities does your organization have for its cyber recovery strategy?

Healthcare organizations that had a material security breach vs. all healthcare respondents

Breached healthcare respondents (N=55)

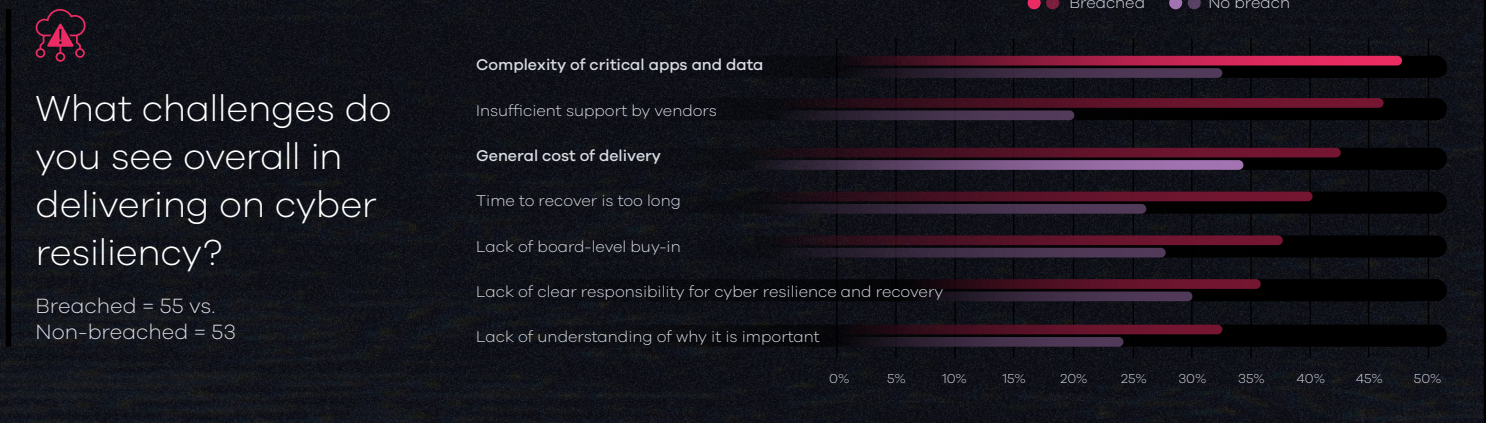


All healthcare respondents (N=63)



When it comes to challenges in delivering on cyber recovery, healthcare organizations that *have* been breached were more likely to cite complexity of critical apps and data as well as insufficient support by vendors (see Figure 2), which was also reflected in anecdotal data from separate interviews with healthcare executives.

Figure 2



This tells us that once an organization has undergone a breach and understands the implications of what it takes to respond, its priorities shift. Those organizations have learned that there are key areas to incorporate that may be less obvious to those that haven't been breached such as: communication with stakeholders, working with vendors, clear ownership, and division of responsibilities.

We spoke with the Chief Medical Information Officer at a large healthcare chain with thousands of locations across the United States. His organization, like so many others, was impacted by the widespread Change Healthcare breach in February, so he understands how going through one can educate you.



"Situations like this is like where you really get to come together as a leadership team and form that trust in relationships, and I think it makes you stronger and more agile for the next time," he says.

"You **don't want these things**, but this is more effective at improving a team than any type of module that would teach you how to do it."

Overall, those that have been breached prepare more comprehensively – they are more likely to have plans, and the plans they do have, they test more frequently. And in response to a breach, they equally prioritize more capabilities and activities vs. trying to do a few things well.

CYBER CHALLENGES TO OVERCOME

In a rapidly evolving landscape of risks, healthcare faces more complexity than other industries.

For security and IT professionals, the risk landscape is constantly evolving, they are particularly concerned about external threats, and organizations must assume breach. Organizations realize it's not a matter of *if* or *when* they will be breached, but a matter of when they find out *that they already have been* breached.

Given this reality, security and IT professionals face a daunting set of challenges. In the overall report, respondents' top security challenges include increasingly sophisticated hackers and attack types, use of artificial intelligence by cybercriminals, a broader attack surface due to cloud and SaaS, and adopting AI-based technologies across security tooling.

On top of all those challenges named, security and IT professionals in healthcare are dealing with extremely sensitive and confidential data, all of which is subject to ever-changing regulations. They are handling protected health information, financial information from patients and employees, identifying information like Social Security numbers, and intellectual property related to medical research.

For large healthcare systems, acquisitions pose another time-consuming challenge: "We do a lot of acquisitions, growth, so remediating those other systems that we take on and converting them to our security policies and putting them on our vendors that have our security protocols, our network, and kind of assessing those risks," the Chief Medical Information Officer says of the process.

Healthcare organizations also rely heavily on third parties to handle information and processes like patient and employee records, laboratory testing, payment processing, or payroll.



"It's really hard to be one of our direct vendors because of how **strict those requirements are with us**, but we can't control the requirements of one of our vendors of how strict they are with someone else. So that's the biggest vulnerability there is," he says.

"We are big enough to have these experts on staff that are our experts to protect us. And I feel very lucky for that."

The Chief Information Security Officer at a large healthcare organization in New York would agree on the challenge of third parties.



“Resiliency can vary because **so many of our processes** are very, very unique and very tied. It’s an entire ecosystem in healthcare,” he says.

“A good portion of our outage from the [CrowdStrike incident in July] wasn’t just the things that hit us directly, like machines that were down, servers that were down; it was also our third parties who we depended on for some of our processes.”

The top cyber recovery challenge named in our survey was the **complexity of critical apps and data**, cited by **44%** of respondents, followed by cost.

A significant number of organizations (**42%**) lack a clear understanding of who is responsible for driving cyber resilience and recovery strategies and execution.

Adoption of several general security capabilities – identity and access management; intrusion protection, detection, and response; data loss prevention/protection; and security posture management – hovers in the **75% to 80% range**, with the current solution in place either satisfactory or in need of improvement.

However, looked at generally,



According to research published in the [Hospital Cyber Resiliency Initiative Landscape Analysis](#), spearheaded by the U.S. Department of Health & Human Services, healthcare organizations are sitting ducks:

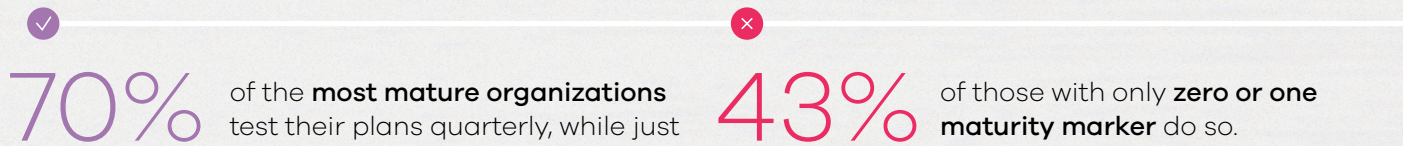
96% of hospitals admit they are running **end-of-life operating systems or software with known vulnerabilities**. While that’s inclusive of medical devices, it is still a stunning number considering how those vulnerabilities are a common target for bad actors.

TESTING IS VITAL TO CYBER RESILIENCE AND READINESS

Frequent cyber recovery testing is a critical practice to improve readiness.

Without testing in a real-world scenario, organizations have no way to know how their cyber recovery plans will perform. We see this when comparing the testing strategies of organizations that have been breached versus those that haven't. Twenty percent of organizations that haven't been breached report they don't test their recovery plan **at all**. That number drops to just 2% for organizations that have been breached.

Additionally, we found that the **most mature organizations prioritize testing** above other measures when planning their cyber recovery strategy.



The bad news for healthcare organizations is that testing remains complicated. The largest systems might have hundreds of locations and hundreds of thousands of users, including large numbers of contingent workers. In situations where workplaces are short-staffed AND frequently dealing with urgent matters, carving out time to focus on testing is hard. Communication and collaboration between siloed organizations is always a challenge, according to the healthcare executives we spoke to.

However, the good news across the **healthcare landscape** is that those organizations indicated in our survey that they



test more frequently than those respondents from **other industries**.

While they need to do so to comply with government regulations, it is commendable that they have been able to prioritize it despite the challenges.

MARKERS OF CYBER MATURITY

Key practices and capabilities mark an organization’s maturity around cyber resilience.

While organizations may cite specific measures as priorities, it’s how they behave that truly matters. When analyzing the most resilient organizations, we found that they employed many measures, but five practices rose to the top when determining their true readiness. We call these practices maturity markers (see [5 Markers of Cyber Recovery Readiness](#), on the next page).

Organizations demonstrating four or five markers are considered cyber mature. These companies report experiencing fewer breaches and recovering faster when they do get breached.

However, our survey found that **only**

10% of healthcare organizations have deployed **all five markers**, and just

19% practice **at least four** (Figure 3).

At the bottom of the maturity curve, **4% have no key markers** in place at all.

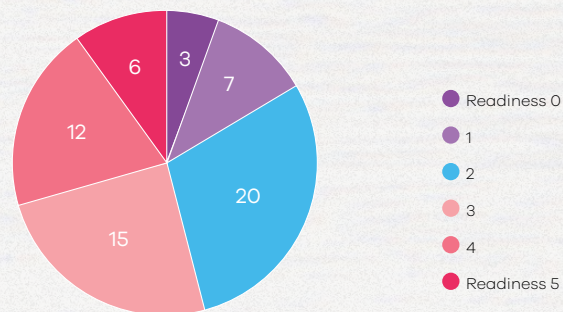
These numbers do compare favorably to the maturity markers indicated by survey respondents across all industries, where only 4% of organizations have deployed all five markers and 14% have no key markers in place at all.

While fewer than half of all organizations feel confident in their recovery plans, more than half of cyber mature healthcare organizations (62%) feel substantially more confident in their ability to recover critical systems and data following a major incident.

Figure 3





What is your organization’s readiness for recovery from security incidents, based on the use of specific capabilities?





5 MARKERS OF CYBER RECOVERY READINESS


An organization's level of cyber maturity can be measured by the presence of five markers. The most mature, cyber-ready organizations demonstrate four or five of these:

-  **1 Security tools to enable early warning about risk, including insider risk.**

Early warning security tools are technologies and systems designed to detect potential cyber threats before they can cause significant harm. These tools aim to identify risks at the earliest possible stage, allowing organizations to respond proactively rather than reactively. Examples include Intrusion Detection Systems, Deception Technology, Intrusion Prevention Systems, Security Information and Event Management, User and Entity Behavior Analytics, and Endpoint Detection and Response.
-  **2 A known-clean dark site or secondary system in place.**

Maintaining an isolated, pre-configured or dynamic isolated recovery environment (for example, a cleanroom) that remains unaffected by cyber incidents at the primary site. This secondary site can be quickly activated for business continuity and data integrity in the event of a cyber attack or major failure. It enhances cyber resiliency by providing a secure failover option, minimizing downtime and complexities of failover.
-  **3 An isolated environment to store an immutable copy of the data.**

Involves maintaining a separate, air-gapped (that is, immutable and indelible) copy of data secured behind a third party's infrastructure. The data remains unchanged and protected from cyber threats, including ransomware and malicious insider actions. It enhances data integrity and availability, providing a reliable recovery option in case of data corruption or loss.
-  **4 Defined runbooks, roles, and processes for incident response.**

A crucial capability for cyber resilience for a structured and efficient response to cyber incidents. Tested runbooks provide step-by-step instructions for handling various types of incidents, reducing confusion and response time. Clearly defined roles and processes ensure that every team member knows their responsibilities, promoting coordinated efforts. This preparedness speeds up recovery and helps maintain operational continuity during and after cyber events.
-  **5 Specific measures to show cyber recovery readiness and risk.**

Metrics and tests that demonstrate an organization's ability to recover from cyber incidents and assess associated risks. These measures, such as regular recovery drills and risk assessments, provide insight into the effectiveness of recovery plans and identify potential vulnerabilities. They are important for cyber resiliency in particular, as well as preparedness, validation of recovery strategies, and to highlight areas for improvement.

CYBER-READY ORGANIZATIONS RECOVER FASTER

Organizations with the most maturity markers are prepared to respond.

As a result of being more prepared, mature healthcare organizations are better positioned to recover from a cyberattack. Unsurprisingly, these companies have more confidence in their ability to recover, with **46% completely confident**.

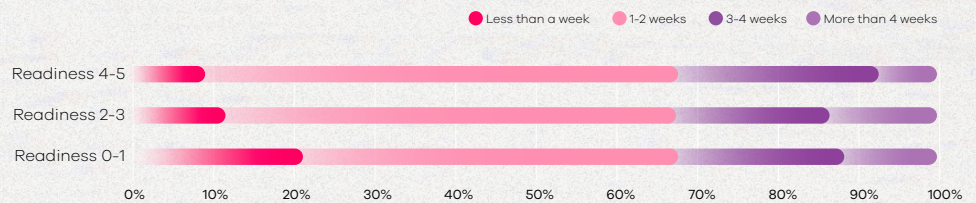
That confidence is warranted: **These mature organizations recover 62% faster than respondents with only zero or one marker and 34% faster than respondents with two or three markers.**

Figure 4



How long did it take your organization to resume normal operations following the breach?

(N=55)



Being offline costs money and can damage a company's reputation and customer trust, so every minute matters. The faster that organizations can resume normal operations, the better. **For healthcare organizations, the stakes are even higher.**

First, let's talk about the financial impact. The cost to remediate a healthcare breach is nearly three times the cost of other industries¹ according to the National Library of Medicine. The average healthcare breach costs nearly \$11 million², while the response to the widespread Change Healthcare breach could cost its parent company \$2.3 billion³.

Reputation and customer trust are important because virtually all people are consumers of healthcare, and nothing could be more personal. Patients rely on healthcare organizations to do no harm – to their wellbeing and the valuable health and financial data to which they are entrusted. It's impossible to put a dollar amount on that.

A PRESCRIPTION FOR PREPAREDNESS

Cyber-ready organizations optimize their people, process, and technology in pursuit of recovery readiness.

It's important to recognize that technology alone cannot improve resilience and readiness. Our research validates the tried-and-true paradigm: **Technology is an enabler of people and processes.**

Most companies recognize that cyber recovery readiness requires a well-rounded approach that accounts for both the resources an organization has and the way that its employees execute.



"The front line of incident prevention and incident response are your people, and performance is driven by company culture," says the Chief Medical Information Officer at a hospital system in Europe.

"Every person being aware of the risks and how to avoid and prevent them, as well as react if/when something happens is both the biggest challenge and the greatest defense. This is **especially true in healthcare** because organizations and technology are extremely complex and frequently changing."

No matter what technology you have in place, you need a culture that values testing and people who know how to execute on a cyber recovery plan when the need arises. Fortunately for the healthcare industry, it's filled with employees who are used to staying calm in emergencies, and who are well-versed in resiliency and recovery.

To learn more about how Commvault can help your organization remain resilient and deliver continuous business, visit our page on [Cyber Recovery in Healthcare](#).



Read the full 2024 Cyber Recovery Readiness Report to see the results across all industries [here >](#)

DEMOGRAPHICS

Figure 1



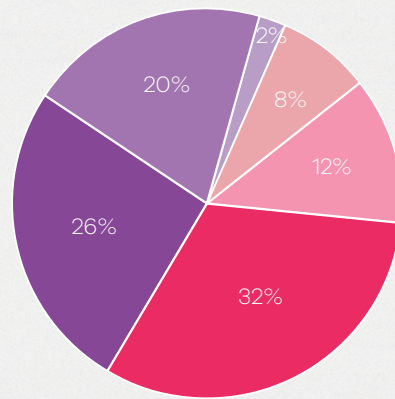
GigaOm conducted this study from 1,000 respondents across 11 countries in April 2024.

Respondents were from companies earning at least \$10 million in annual revenues, with the **majority earning \$500 million or more.**

Thirty-five percent of respondents were board-level or C-Suite executives, **48% were senior-level management**, and the remaining 17% were mid- or junior-level management.

Sixty-three respondents worked in healthcare; 43 at large healthcare organizations (more than 5,000 employees).

- \$25M - \$100M
- \$500M - \$1B
- \$5B - \$50B
- \$100M - \$500M
- \$1B - \$5B
- More than \$50B



- Board member; C-level
- Mid-level management
- Senior management
- Junior management

