



# WHAT WE LEARNED FROM 1,000 IT EXPERTS

CYBER RECOVERY  
READINESS REPORT

2024

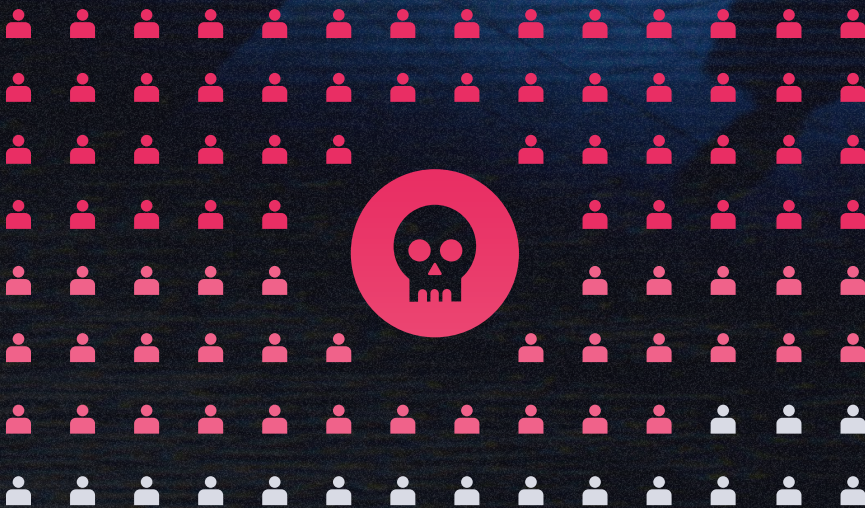
 Commvault®

In partnership with **GIGAOM**

# ARE YOU READY?

We recently partnered with GigaOm to survey 1,000 global cybersecurity and IT leaders on the evolving landscape of cyber resilience.

We uncovered a stark reality:



83%

of organizations have experienced a **material security breach**, with over

50%

occurring in the **past year** alone.

This prevalence underscores the urgent need for robust cyber recovery strategies that require a broader spectrum for practices that go beyond traditional disaster recovery plans.

Read on to find out more about the steps your organization should take.

# CONTENTS

A Breach Can Teach	4
Cyber Challenges to Overcome	6
5 Markers of Cyber Recovery Readiness	7
Preparation Pays Off	8
Cyber Recovery Goes Beyond Disaster Recovery	9
Testing Is Vital to Cyber Resilience and Readiness	10
Summary	11

# A BREACH CAN TEACH

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

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. With breaches costing up to \$12 million per day<sup>1</sup>, the ability to recover quickly is paramount.

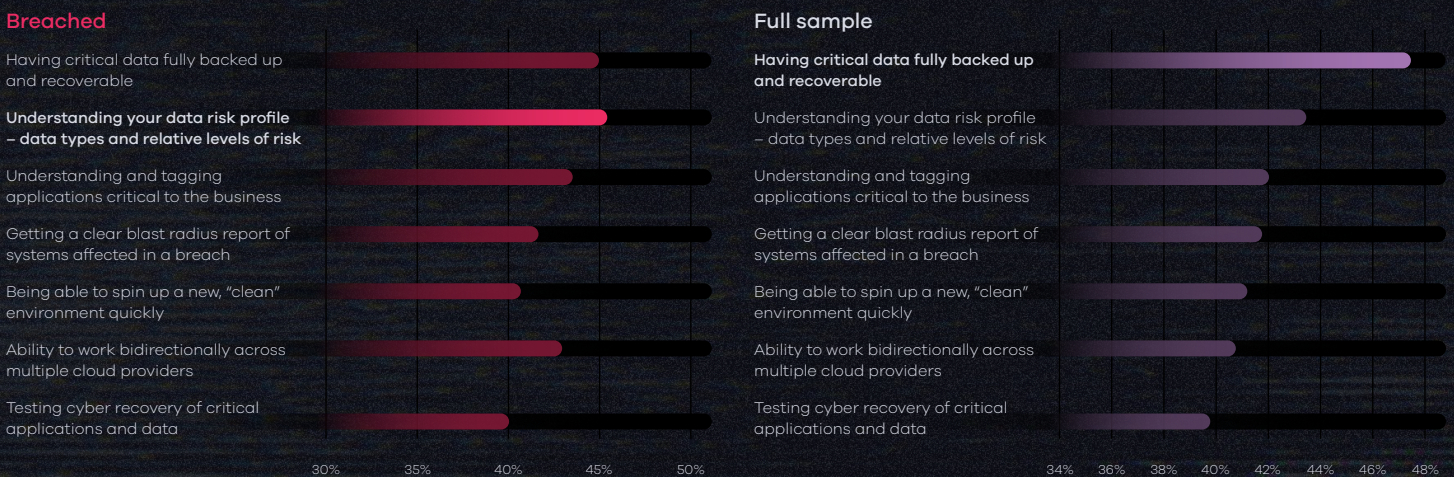
One significant finding across the data set is that there are many lessons to be learned from being breached. Organizations that experienced a breach are nearly 2.5 times more likely to rank understanding data risk profile, data classifications, and relative level of risk as a top priority for their 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?

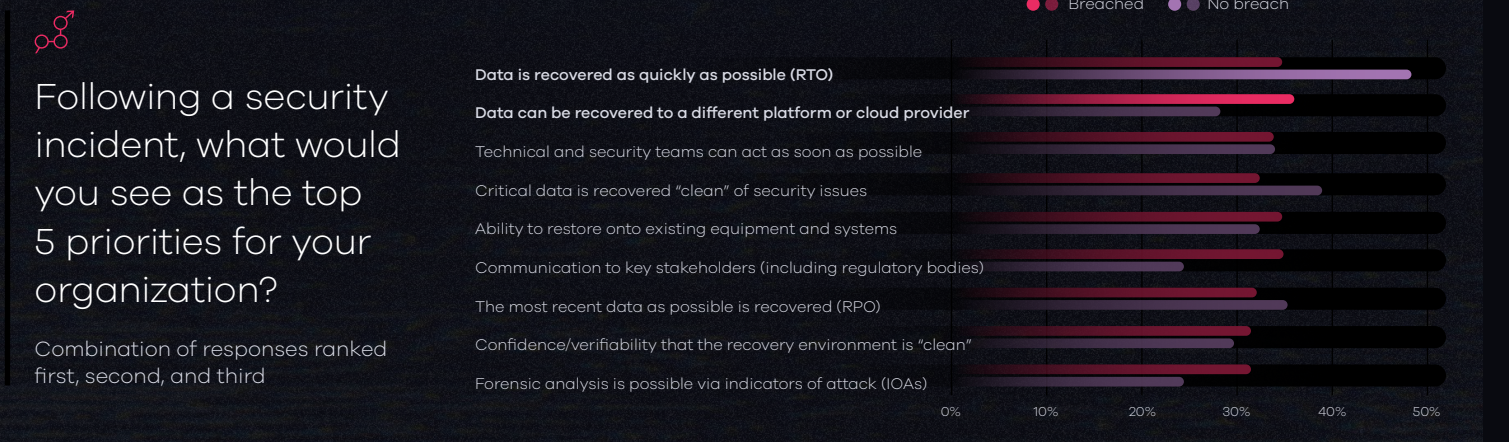
Organizations that had a material security breach vs. all respondents



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. Those that haven't been breached are primarily focused on speed alone.

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 (Figure 2).

Figure 2



# CYBER CHALLENGES TO OVERCOME

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.

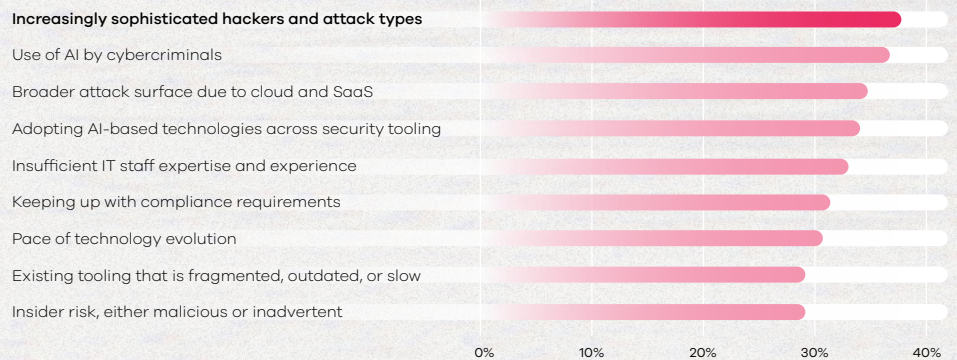
For security and IT professionals, the risk landscape is constantly evolving, they are particularly concerned about external threats, and organizations must assume breach.

Given this reality, security and IT professionals face a daunting set of security challenges (Figure 3). As for cyber recovery challenges, the complexity of critical apps and data was cited by 44% of respondents. A significant number of organizations (42%) lack a clear understanding of who is responsible for driving cyber resilience and recovery strategies and execution.

Figure 3








What do you see as the biggest challenges to your organization's cybersecurity posture?



# 5 MARKERS OF CYBER RECOVERY READINESS

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. The most mature, cyber-ready organizations demonstrate four or five of these:

-  1 Security tools to enable early warning about risk, including insider risk.
-  2 A known-clean dark site or secondary system in place.
-  3 An isolated environment to store an immutable copy of the data.
-  4 Defined runbooks, roles, and processes for incident response.
-  5 Specific measures – such as regular recovery drills and risk assessments – to show cyber recovery readiness and risk.

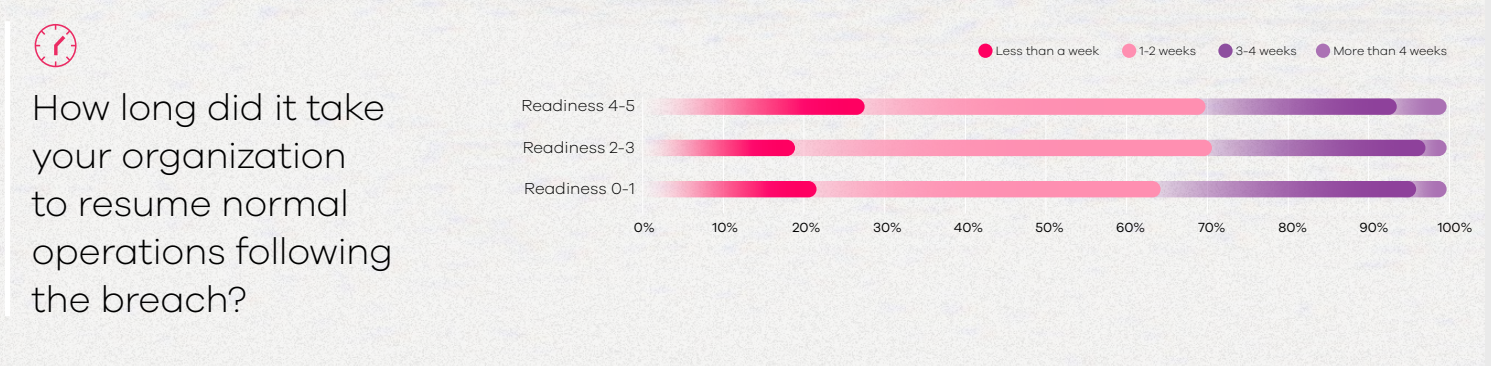
# PREPARATION PAYS OFF

The most mature organizations prioritize testing and backup of critical data, but also put near-equal importance on the ability to work across multiple cloud providers, understanding and tagging business-critical applications, and quickly spinning up a clean environment.

The result is a stronger security posture and better cyber resilience. Overall, they are about half as likely to experience a breach as less mature companies.

Unsurprisingly, these mature companies have more confidence in their ability to recover, with 54% completely confident. In fact, these organizations recover 41% faster than respondents with only zero or one marker and 24% faster than respondents with two or three markers (Figure 4).

Figure 4



In addition, those that had already completely or partially adopted a recovery plan typically also recover 41% faster than those that don't have a plan.



# CYBER RECOVERY GOES BEYOND DISASTER RECOVERY

It's important to note that while some companies prepare for cyber recovery as an element of an overall disaster recovery plan, cyber recovery is not the same as disaster recovery.

Disaster recovery plans are created in anticipation of more predictable events like hardware failures or natural disasters like fires and floods. While these kinds of events are certainly devastating, companies are usually able to get back online more quickly because they are following the steps of a predefined plan. Importantly, in a natural disaster, the data can likely be trusted. So, disaster recovery can focus on data integrity, speed of recovery, and meeting established recovery objectives.

Cyber events are different. In a cyberattack, the data cannot be trusted. So, recovery plans must include the important elements of recovering cleanly and reliably so recovery doesn't make matters worse. Cyber recovery plans should include Zero Trust recovery mechanisms.

Respondents recognize this important difference. In our survey, over 90% of respondents say that their organization manages disaster recovery separately from cyber recovery, which is a sign most companies acknowledge the differences and prepare for them accordingly.

# TESTING IS VITAL TO CYBER RESILIENCE AND READINESS

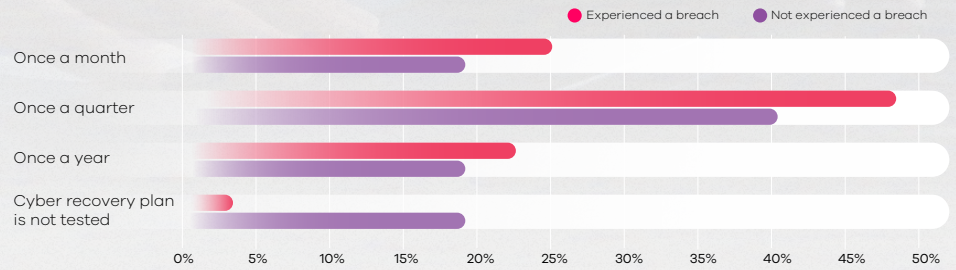
Without testing in a real-world scenario, organizations have no way to know how their cyber recovery plans will perform.

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** (Figure 5). That number drops to just 2% for organizations that have been breached.

Figure 5



How often is your organization's cyber recovery plan tested?

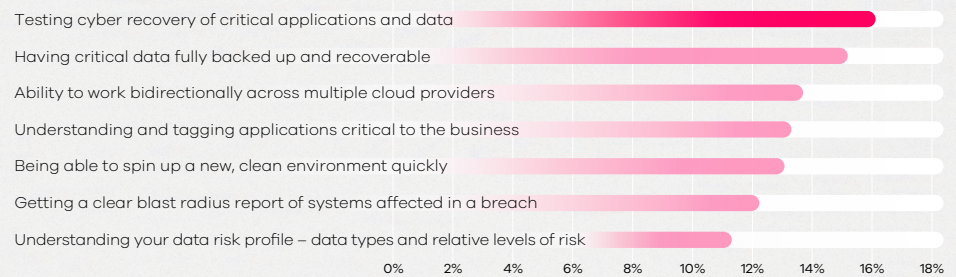


Additionally, we found that the most **mature organizations prioritize testing** above other measures when planning their cyber recovery strategy (Figure 6). Seventy percent of the most mature organizations test their plans quarterly, while just 43% of those with only zero or one maturity marker do so (Figure 7).

Figure 6



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

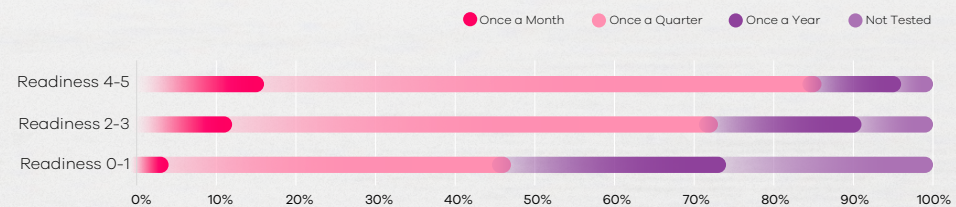


Note: Organizations with 4 or 5 maturity markers

Figure 7



How often does your organization test its cyber recovery plan?



# SUMMARY

## The State of Cyber Recovery Readiness

The results of our survey provide substantial evidence of a **divide in perspective between those that have suffered a breach and those that have yet to suffer a breach**. But actions speak louder than word: Organizations will have to change their behaviors to improve their chances of successfully navigating a breach and restoring their systems and data.

Working on a plan to reach the five markers of cyber resiliency will make your organization better prepared. Investing in a testing regimen, and helping everyone understand their role in it, will increase your overall chances of successfully navigating a cyberattack.

Download the full report [here](#).

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