CYBER RECOVERY READINESS REPORT

2024

Commvault®

In partnership with GIGAOM

Dear Reader,

Welcome to a pivotal moment in the evolution of cyber resilience. Since the inception of The Collaborative in early 2024, our mission has been clear: to forge strong partnerships with analysts, industry leaders, and visionaries like you, to deeply explore and enhance cyber resilience across diverse organizations. Our foundational report, "Seven Emerging Trends in Cyber Resilience," has already set the agenda for this year, addressing critical areas as we confront the escalating ransomware menace.

We are excited to announce the release of the 2024 Cyber Recovery Readiness Report, a collaboration between Commvault and GigaOm. Your leadership and expertise in IT and security are crucial in steering the future toward enhanced cyber resilience. This report is crafted to equip you with essential insights and data, empowering your organization to stay ahead in an increasingly volatile cyber landscape.

The insights we share are derived from an extensive survey of 1,000 global cybersecurity and IT leaders. This report not only offers a worldwide view of the challenges but also pinpoints effective strategies essential for cyber recovery readiness. It underscores the critical need for comprehensive cyber recovery strategies that surpass traditional disaster recovery plans.

Key Findings:

- A staggering 83% of organizations have suffered a material security breach recently, with over half occurring in the past year alone, underscoring the critical need for advanced preparedness and agile response strategies.
- The most resilient organizations share common practices that significantly enhance their recovery readiness. Our analysis reveals that the most prepared organizations exhibit at least four out of five key markers of maturity.
- There is a clear correlation between cyber maturity and recovery speed. Organizations with higher levels of cyber maturity recover from breaches 41% faster than those less prepared.
- Regular testing of cyber recovery plans is not just beneficial; it is essential. Our data shows a marked difference in testing frequency between organizations that have experienced breaches and those that have not.

Recommendations:

1. Regularly test and enhance your recovery plans. Frequent drills and updates ensure that your organization can respond swiftly and effectively to any cyber incident.
2. Prioritize building cyber maturity by adopting the identified markers of cyber recovery readiness. This not only mitigates risks but significantly lessens the impact of potential breaches.
3. Develop a holistic cyber recovery strategy that extends beyond mere data backup to encompass full system recovery, ensuring comprehensive business continuity.

We invite you to delve into the report and integrate these insights and recommendations into your strategic planning. Our goal is not merely to inform but to inspire decisive action that will robustly fortify your organization against future cyber threats.

We are here to support you on this journey toward unparalleled cyber recovery readiness.

Thankfully,

The Collaborative

CONTENTS

A BREACH CAN TEACH

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

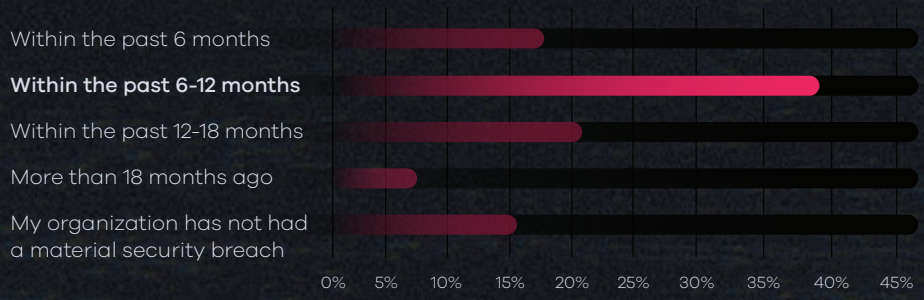
Unfortunately, breaches are far too common, affecting companies of all sizes across all industries. Like any dramatic experience, the experience of fighting through a breach reshapes how an organization behaves and prioritizes its actions. These were among the findings in our inaugural Cyber Recovery Readiness Report, a joint effort of Commvault and GigaOm.

We 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. See more details about our methodology and respondents on Page 17.

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 (Figure 1). With breaches costing up to **$12 million per day**, the ability to recover quickly is paramount[1]

Figure 1

When was your organization's last material security breach?



83% of our sample reported a material security breach, with over **50%** of these within the **past year.**

  1 SolarWinds: Pingdom Team, Average Cost of Downtime per Industry, Jan 9, 2023.

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, 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 2).

Figure 2

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

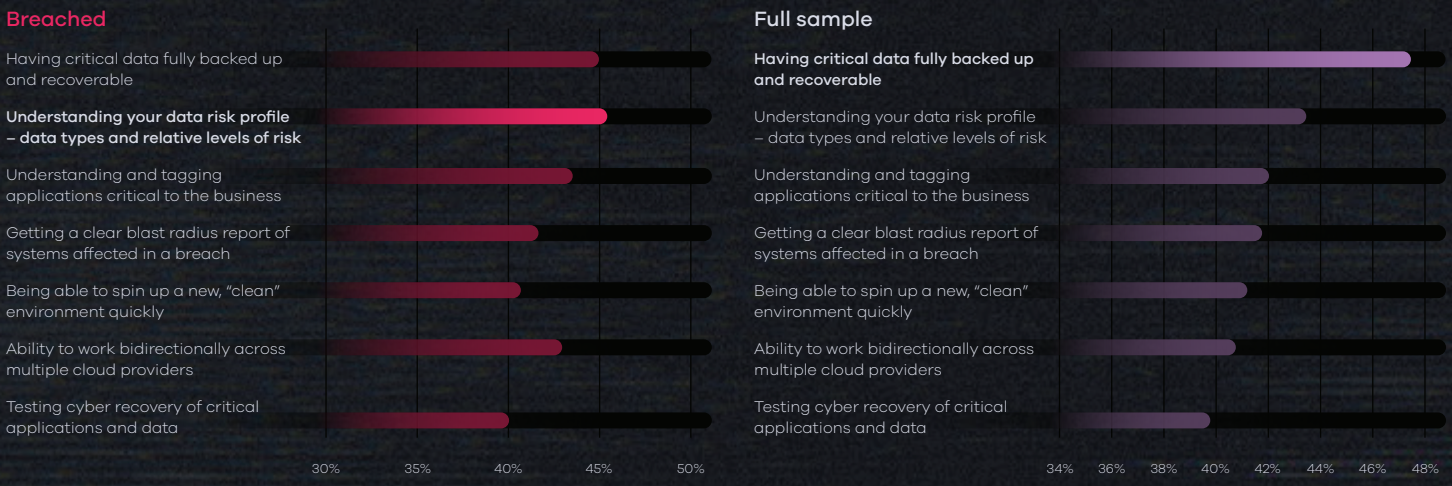
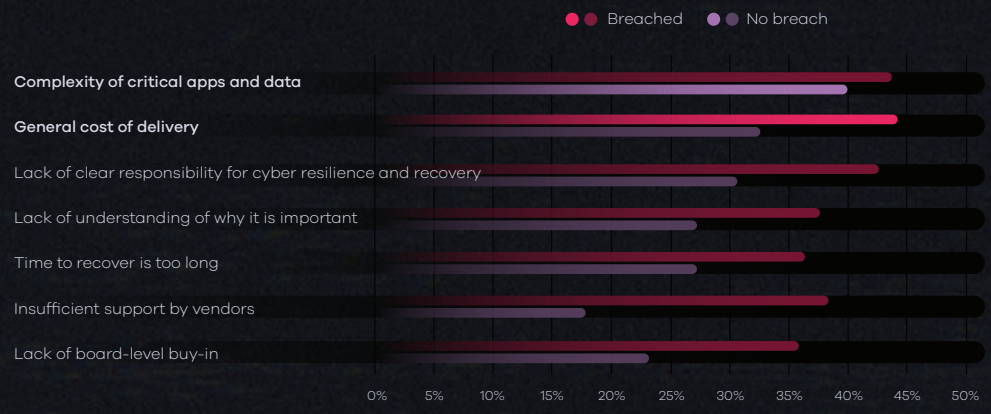


Figure 3

What challenges do you see overall in delivering on cyber resiliency?

Data split: Have you been breached?



Overall, organizations that haven't been breached have a narrower focus, citing the need to have critical data fully backed up and recoverable as a top three choice nearly 60% of the time (Figure 3). Organizations that have been breached place a premium on a wider set of practices, led by understanding their data risk profile and classifications.

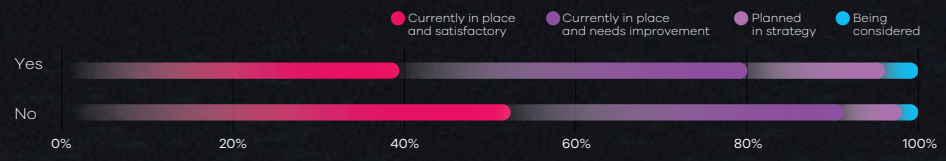
This tells us that once an organization has undergone a breach and understands the implications of what it takes to respond, its priorities shift. Those organizations have learned that there are key areas to incorporate that may be less obvious to those that haven't been breached such as: communication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

Breached organizations are also less satisfied with the status of their early warning tools compared to those that did not report a breach (Figure 4), suggesting a level of complacency in the unbreached group.

Figure 4

To what extent does your organization have the following capabilities in place for recovery from security incidents?

Specific measures to show cyber recovery readiness and risk vs. breached

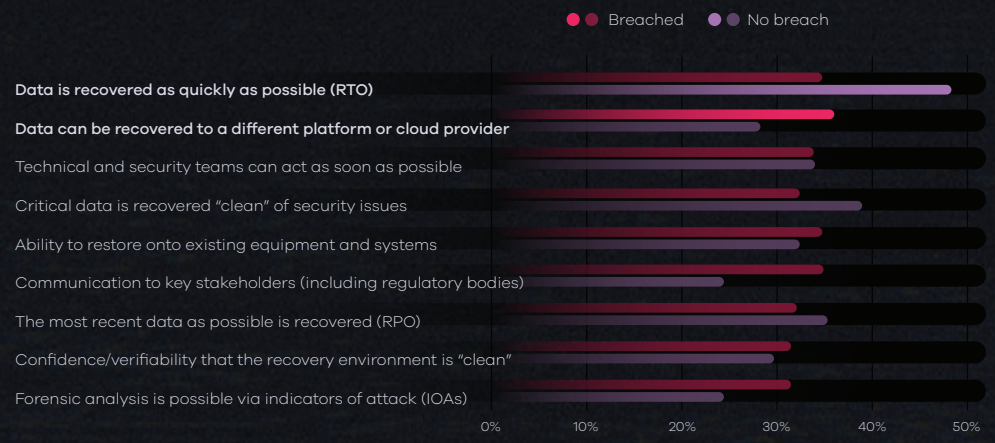


Overall, those that have been breached prepare more comprehensively – they are more likely to have plans, and the plans they do have, they test more frequently. And in response to a breach, they equally prioritize more capabilities and activities vs. trying to do a few things well (Figure 5).

Figure 5

Following a security incident, what would you see as the top 5 priorities for your organization?

Combination of responses ranked first, second, and third



CYBER CHALLENGES TO OVERCOME

In a rapidly evolving landscape of risks, organizations prioritize protecting data.

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. 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 (Figure 6).

Figure 6

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

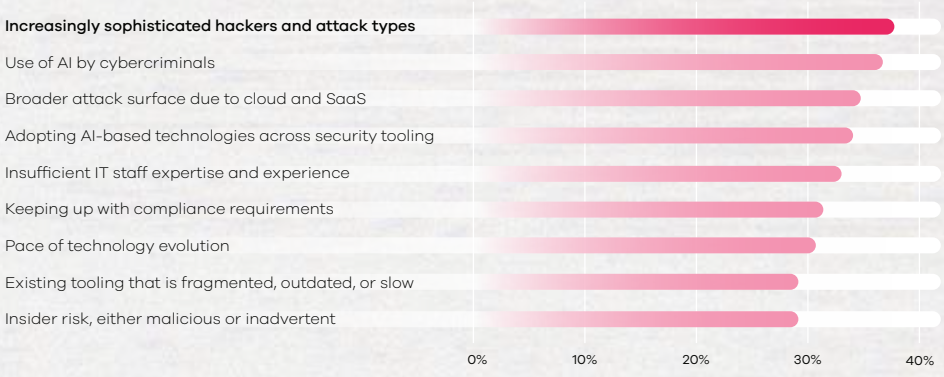
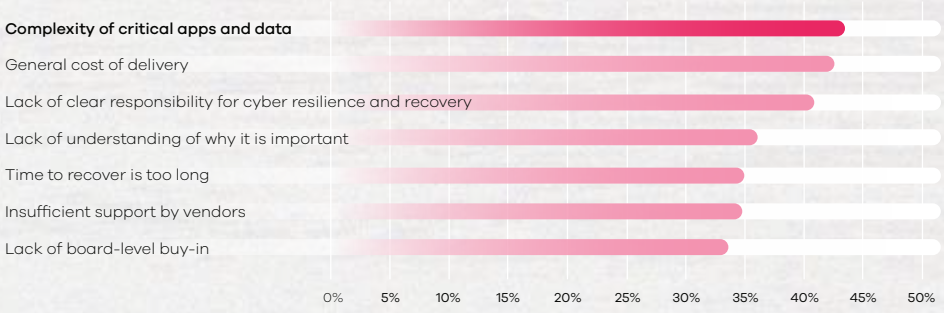


Figure 7

What challenges do you see overall in delivering on cyber recovery?



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 (Figure 7).

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 (Figure 8).

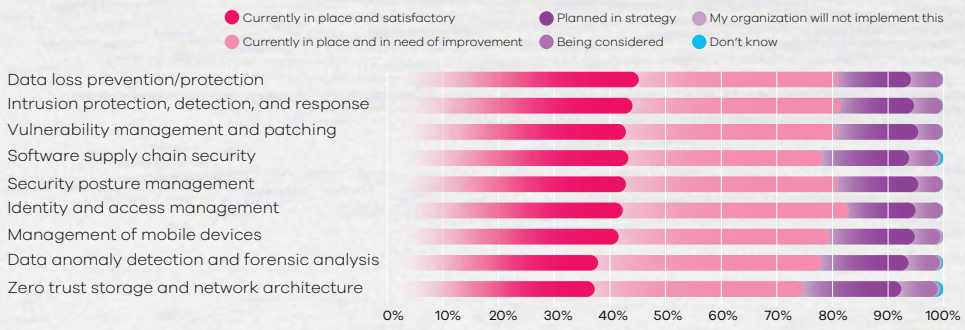
However, looked at generally,

42% of respondents are **satisfied** with their general cybersecurity, while

38% see a **need for improvement** to their cybersecurity measures.

Figure 8

To what extent have the following key elements of your organization's cybersecurity architecture been adopted and/or implemented?



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, Page 9).

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 4% of organizations have deployed all five markers, and just 13% practice at least four. At the bottom of the maturity curve, 14% have no key markers in place at all (Figure 9).

While fewer than half of all organizations feel confident in their recovery plans (Figure 10), more than half of cyber mature organizations (54%) feel substantially more confident in their ability to recover critical systems and data following a major incident (Figure 13, Page 11).

Figure 9

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

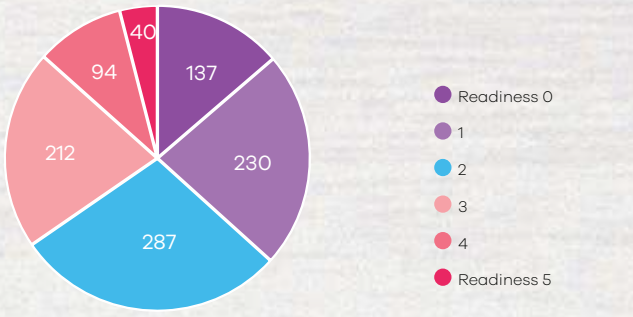
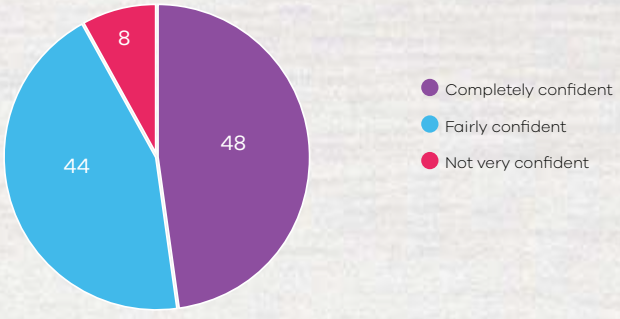


Figure 10

How confident are you that you have a solid recovery plan in place, specific to cybersecurity threats?



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.

DON'T CUT CORNERS

Cyber-ready organizations take no shortcuts when it comes to cyber resilience and readiness.

For many organizations, cyber recovery strategy is still a work in progress. Again, 38% of our respondents recognize that their efforts could use improvement.

Those aiming to improve should look to their more mature peers, which place a premium on prioritizing more practices vs. just a few, and, as a result, are on more solid footing in the face of a breach.

They 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 (Figure 11).

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 (Figure 12).

Figure 11

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

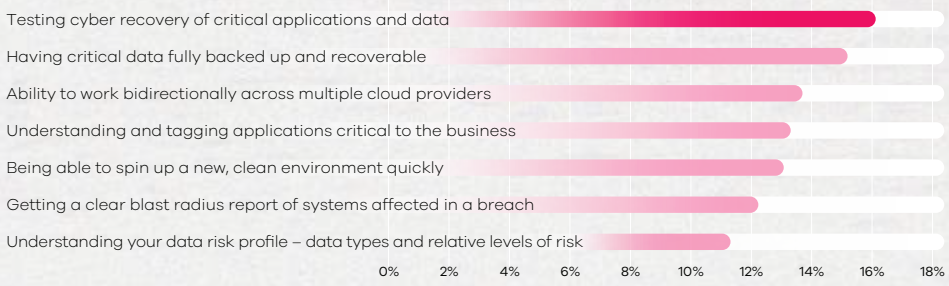
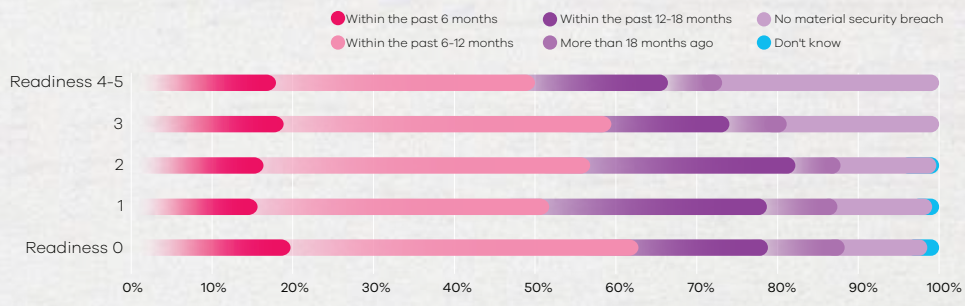


Figure 12

When was your organization's last material security breach?



CYBER-READY ORGANIZATIONS RECOVER FASTER

Organizations with the most maturity markers are prepared to respond.

As a result of being more prepared, mature organizations are better positioned to recover from a cyberattack. Unsurprisingly, these companies have more confidence in their ability to recover, with 54% completely confident (Figure 13).

That confidence is warranted: **These mature organizations recover 41% faster than respondents with only zero or one marker and 24% faster than respondents with two or three markers** (Figure 14).

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.

Figure 13

To what extent are you confident your organization can recover critical systems and data following a major incident?

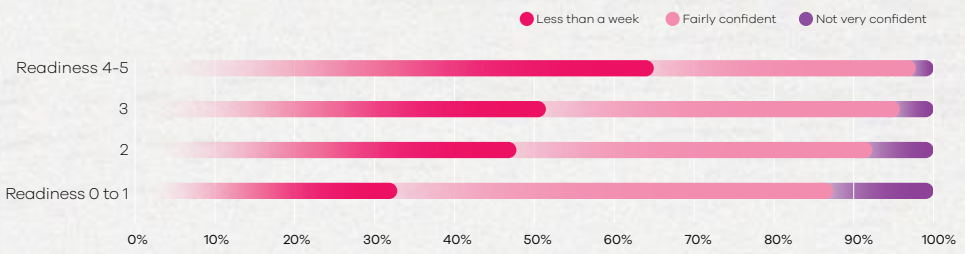
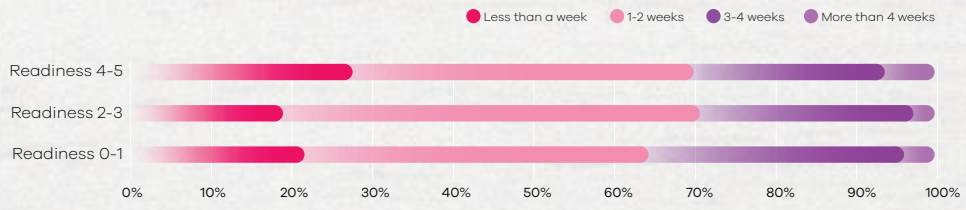


Figure 14

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



CYBER RECOVERY GOES BEYOND DISASTER RECOVERY

Traditional disaster recovery doesn't suffice when recovering from a cyber incident.

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**.

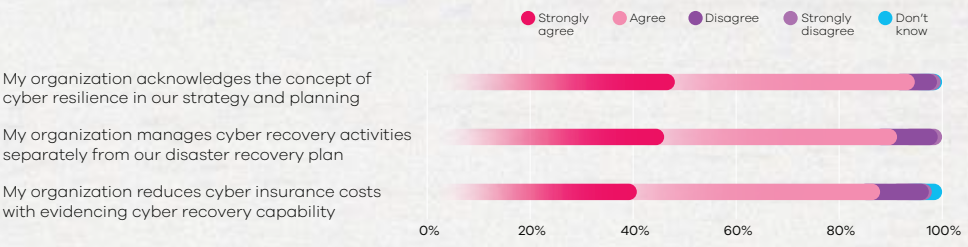
Disaster recovery plans are created in anticipation of more predictable events like hardware failures or natural disasters like fires and floods. While these kinds of events are certainly devastating, companies are usually able to get back online more quickly because they are following the steps of a 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** (Figure 15), which is a sign most companies acknowledge the differences and prepare for them accordingly.

Figure 15

To what extent do you agree or disagree with the following statements?



RECOVERY READINESS REQUIRES CAPABILITIES, COMPETENCIES, AND CULTURE

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 their company has and the way that their employees execute.

Capabilities: the tools and systems an organization has in place to recover after a breach.

Competencies: the capacity and ability of an organization to execute on their capabilities effectively and efficiently.

Culture: an organization's values and ability to put them into practice.

If capabilities are a company's "hard skills," culture encompasses its "soft skills." How often do they test? How much value do they place on investing in both tools and the time to test them? How well do employees collaborate and communicate to execute on a rigorous testing regimen? All these factors affect how prepared a company is to face cyber threats.

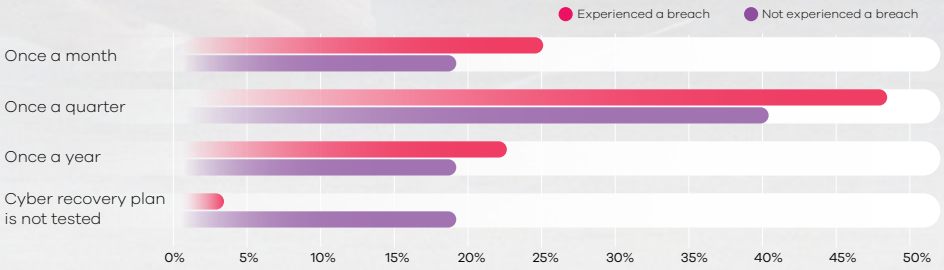
TESTING IS VITAL TO CYBER RESILIENCE AND READINESS

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*** (Figure 16). That number drops to just 2% for organizations that have been breached.

Figure 16

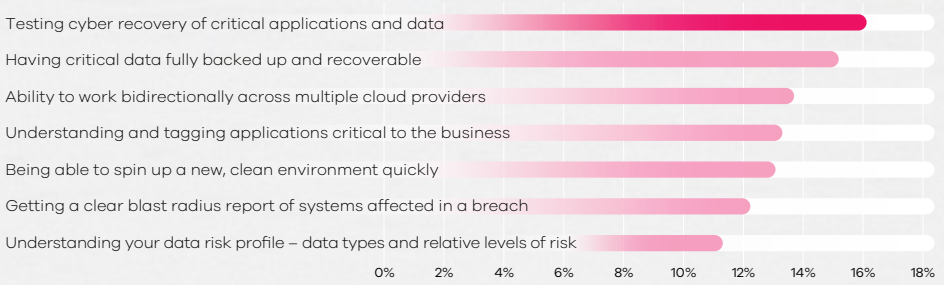
How often is your organization's cyber recovery plan tested?



Additionally, we found that the **most mature organizations prioritize testing** above other measures when planning their cyber recovery strategy (Figure 17). 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 18).

Figure 17

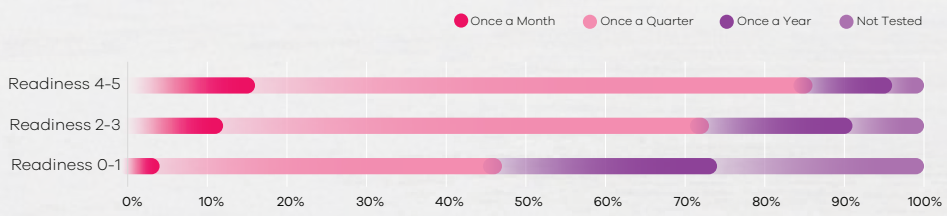
In response to security incidents, what priorities does your organization have for its cyber recovery strategy?



Note: Organizations with 4 or 5 maturity markers

Figure 18

How often does your organization test its cyber recovery plan?



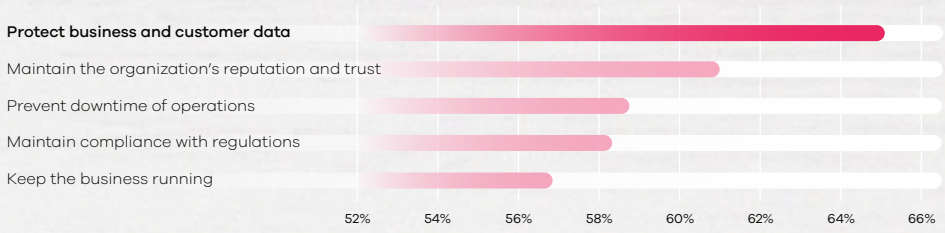
WHY READINESS MATTERS – MITIGATING THE IMPACT OF A BREACH

Readiness gives organizations the confidence to remain resilient through an attack.

Breaches are not only common but also threaten a company's resources and brand. Through the survey we learned that the overwhelming security priority for organizations is protecting business and customer data, followed by maintaining the organization's reputation and trust (Figure 19).

Figure 19

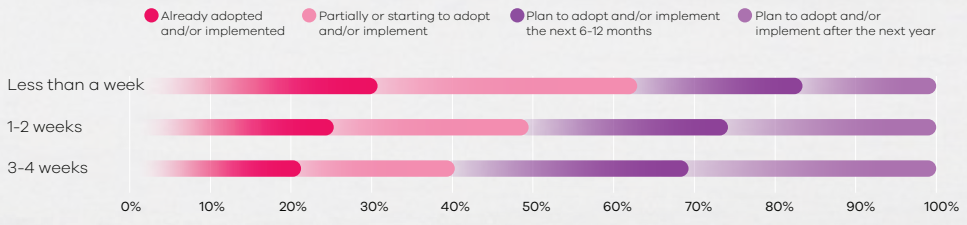
What are your organization's most significant security priorities from a business perspective?



These attacks have an obvious impact on the usual course of business. We found that **those that had already completely or partially adopted a recovery plan** typically **recover 41% faster** than those that don't have a plan (Figure 20).

Figure 20

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



This is why confidence in cyber recovery readiness is of the utmost importance. Those with the most maturity markers are nearly twice as confident in their cyber resilience posture than those with only zero or one marker (Figure 13, Page 11). That readiness is what helps mature organizations recover faster from a breach and incur fewer breaches overall.

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 it's important to remember that actions speak louder than words. It's not enough to say you will behave differently. Organizations will have to change their behaviors to improve their chances of successfully navigating a breach and restoring their systems and data.

If you are among the **38% who feel their cyber security measures could use improvement** or you're in the majority who **doesn't feel fully confident in your ability to recover after a breach**, there are actions you can take.

Ensuring your organization has a plan to **reach the five markers of cyber resiliency** will make you better prepared. Investing in a testing regimen, and making sure everyone understands their role in it, will increase your overall chances of successfully navigating a cyberattack.

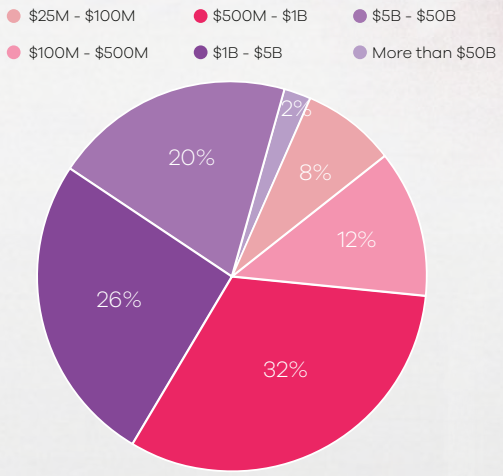
You can't rest on your laurels and operate under the delusion that you're immune from danger. **Understanding and acknowledging the risks empowers you to come through a breach with your data – and reputation – intact.**

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.