

2024

CYBER RECOVERY READINESS REPORT

KEY FINDINGS


We partnered with GigaOm, surveying **1,000 cybersecurity and IT leaders** from across the globe in order to gain critical insights and actionable intelligence to guide you through the evolving landscape of cyber resilience.

Here's what we learned:


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:


- 01**




Security tools to enable early warning about risk, including insider risk.
- 02**



A known-clean dark site or secondary system in place.
- 03**



An isolated environment to store an immutable copy of the data.
- 04**



Defined runbooks, roles, and processes for incident response.
- 05**



Specific measures, such as regular recovery drills and risk assessments, to show cyber recovery readiness and risk.

Mature organizations with **4-5 markers** of cyber resiliency recover

41% faster

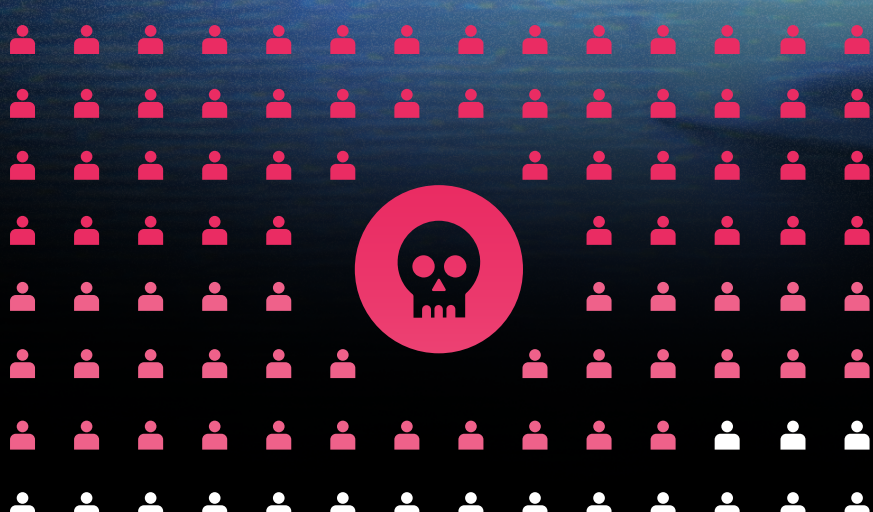
than those with **0 or 1 marker**, and

24% faster

than those with **2 or 3 markers**.

Only **4%** of surveyed organizations have deployed **all five markers**.

A BREACH CAN TEACH



83%

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

50%

within the **past year**.

RESILIENCE AFTER A BREACH

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



Breached organizations prioritize a **broader set of practices** and are nearly

2.5x more likely

to rank understanding data risk profiles as a top priority.

Source: 2024 Cyber Recovery Readiness Report by Commvault and GigaOm

Download the full report to learn more about global cyber resilience challenges and data-driven strategies for cyber recovery readiness.