

# Cyber Resilience Insights

Exploring cyber resilience gaps, evolving threats, AI-driven defenses, and recovery strategies in APJ

Cyber resilience challenges are intensifying as cyberattacks and data protection gaps drive increased risks of disruption. Organizations with mature resilience strategies\* are nearly three times more likely to recover successfully. By modernizing resilience strategies, enhancing detection capabilities, and prioritizing continuous optimization, IT leaders can minimize risks and strengthen confidence in their ability to adapt to evolving threats.

## Leadership Overconfidence

**74% of IT professionals believe their leadership overestimates cyber event readiness.** When overconfidence takes the wheel, it creates dangerous blind spots that delay critical investments and leave vulnerabilities unaddressed.



## The Confidence vs. Capability Gap

**99.3%**

of organizations have cyber resilience strategies in place

Yet **55%**

failed to recover effectively from their last test or incident

## Prevention vs. Recovery: An Unbalanced Approach

**87%**

believe their organization focuses more on preventing attacks than preparing to recover from them

Yet only

**30%**

have a comprehensive platform for threat detection across primary storage, backup storage and network infrastructure

And only

**41%**

successfully contained and recovered from an attack or cyber incident drill with minimal impact

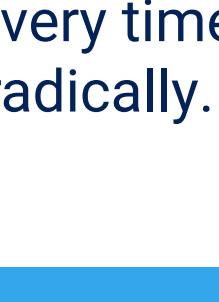
Consequently, when breaches inevitably occur, many organizations are unprepared for the recovery phase that determines business survival.

## The Path Forward:

Mature Organizations Deliver Results

**Organizations with mature cyber resilience strategies are nearly 2.8x more likely to recover successfully**

Strategic maturity across three essential pillars work together to create unbreakable resilience.



**SECURE:**

Building Your Foundation of Trust

Organizations with mature cyber resilience strategies are:

**1.8x more likely** to protect devices using firmware/BIOS-level security controls

**More likely** to leverage encryption for data at rest and in transit

**More likely** to utilize cyber vaults to protect critical data from evolving threats

But security is just the beginning. The real advantage comes from intelligent detection that spots threats before they compromise your most valuable assets.



**DETECT:**

Intelligence That Never Sleeps

### The Visibility Challenge:

Only 30% of organizations have robust threat detection across backup storage, primary data storage, and network infrastructure

### The AI-Powered Solution:

**57%** are prioritizing investments in AI/ML-powered threat detection

**52%** extensively scan backup data with AI/ML for indicators of compromise

Organizations with mature strategies are **2.3x more likely** to use AI/ML tools with proactive mitigation and responsive playbooks



**RECOVER:**

Where Preparation Meets Performance

### The Testing Advantage:

**61%** of organizations conducting monthly or more frequently simulated cyberattacks successfully recovered from incidents

**59%** of organizations testing less than monthly did not successfully recover from incidents

### The Result:

Organizations that test frequently are significantly more likely to meet both recovery time objectives and recovery point objectives than those that test sporadically.

Organizations with mature cyber resilience strategies are 2.3x more likely to consistently meet their SLAs

### Building Your Robust Foundation

Prioritize both prevention and rapid recovery.

**Secure:** Reduce risk with BIOS-level security controls, data encryption, and cyber vaults for critical data.

**Detect:** Use real-time AI/ML to detect and respond to threats across all storage, including primary and backup storage.

**Recover:** Test recovery often—organizations that do so monthly are far more likely to meet recovery objectives.

## Ready to enhance your cyber resilience?

Ready to enhance your cyber resilience? Read all the key findings from the [Dell 2026 Cyber Resilience Research](#).

**DELL** Technologies

Source: Varian Bourne and Dell Technologies Cyber Resilience Survey 2025. Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Copyright © Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. \*Organizations with mature cyber resilience strategies are defined as those with a strategy that is fully established and continuously optimized, using predictive analytics, automation, and real-time insights (e.g., threat intelligence feeds, ML-driven cyber resilience strategies) and are improved as they are used.