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.

69% of IT professionals believe their

Leadership Overconfidence

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%

cyber resilience strategies in place

of organizations have

53%

effectively from their last test or incident

failed to recover

Prevention vs. Recovery: An Unbalanced Approach

86% believe their organization focuses

more on preventing attacks than preparing to recover from them

36% have a comprehensive

Yet only

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

46%

And only

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

unprepared for the recovery phase that determines business survival.

Consequently, when breaches inevitably occur, many organizations are

Mature Organizations Deliver Results

likely to recover successfully

The Path Forward:

Organizations with mature cyber resilience strategies are nearly 3x more

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

SECURE:



2x more likely to protect

devices using

Organizations with mature cyber resilience strategies are:

Building Your Foundation of Trust

and in transit firmware/BIOS-level security controls

DETECT:

spots threats before they compromise your most valuable assets.

But security is just the beginning. The real advantage comes from intelligent detection that

More likely to leverage

encryption for data at rest

More likely to utilize

threats

cyber vaults to protect

critical data from evolving

Intelligence That Never Sleeps



storage, and network infrastructure The AI-Powered Solution:

62% extensively scan

backup data with AI/ML for

indicators of compromise

investments in AI/ML-powered threat detection

65% are prioritizing





Where Preparation Meets Performance

Organizations with

AI/ML tools with

mature strategies are

3.2x more likely to use

proactive mitigation and

response playbooks

monthly or more frequently simulated cyberattacks successfully recovered from incidents

The Testing Advantage:

The Result: sporadically.

61% of organizations conducting

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

from incidents

60% of organizations testing less than

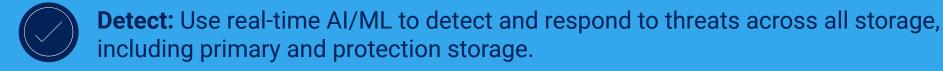
monthly did not successfully recover

Your Path to Cyber Resilience Excellence Organizations with mature cyber resilience strategies are 2.3x more likely to

Building Your Robust Foundation

consistently meet their SLAs

Prioritize both prevention and rapid recovery.



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



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

Dell 2025 Cyber Resilience Insights Research.

Ready to enhance your cyber resilience?

Ready to enhance your cyber resilience? Read all the key findings from the

D¢LLTechnologies