Cyber Resilience Insights

Benchmarking U.S. Enterprise Readiness Across Secure / Detect / Recover
Insight Discussion
August 2025

DELL Technologies

Agenda

- Objectives and Firmographics
- The Cyber Resilience Gap
- Secure
- Detect
- Recover
- Complexity, Culture and What’s Next

Business objectives

- To position Dell as a thought leader and strategic partner for cyber resilience
- To reaffirm the decision to move away from the “data protection” label into “cyber resilience”

Research objectives

- Assess the maturity and integration of cyber resilience strategies
- Evaluate the effectiveness of organizations’ secure, detect and recovery practices
- Understand barriers to improving cyber resilience, including skill gaps, budget, and complexity
- Explore how organizations are securing their IT environment and protecting data from ransomware threats

Who did we interview?

Respondents were interviewed in July 2025

200 IT decision makers from US organizations

Organizations with 1,000 + employees

Organizations from a range of public and private industries

Respondents are:
Board members; C-level
Senior managers
Mid-level managers

Key findings

54%

of organizations have a fully established and continuously optimized cyber resilience strategy

Continuous optimization is key - without it, strategies can quickly become outdated against evolving threats leaving organizations at greater risk

59%

recognize their backup data is not as well protected as it should be

Strengthening backup protection is essential to ensure recovery remains possible when primary systems are compromised.

Secure

36%

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

Without unified detection, threat visibility and response times can be slower, increasing the risk of undetected breaches.

Detect

61%

of those who conducted simulated cyberattacks monthly or more frequently successfully recovered from a drill/cyber incident

Frequent testing helps teams prepare for the real deal. Teams that are unprepared risk delayed response and recovery when it matters most.

Recover

69%

think leadership overestimates their organization’s readiness for a major cyber event

Overconfidence can stall investments, delay response planning, and leave critical vulnerabilities unaddressed

Section 1: The Cyber Resilience Gap

Understanding the problem and the urgency to evolve

Continuously optimizing resilience strategies improves recovery, yet success is not guaranteed

99% have a cyber resilience strategy of some form

54% believe it to be fully established and continuously optimized (a mature strategy)

53% did not contain and recover effectively during their last test or incident

Organizations with mature resilience strategies are nearly **3X more likely to recover** successfully **(65% vs 24%)**

69% believe **leadership overestimates their readiness** for a major cyber event

DELL Technologies

Why this matters now

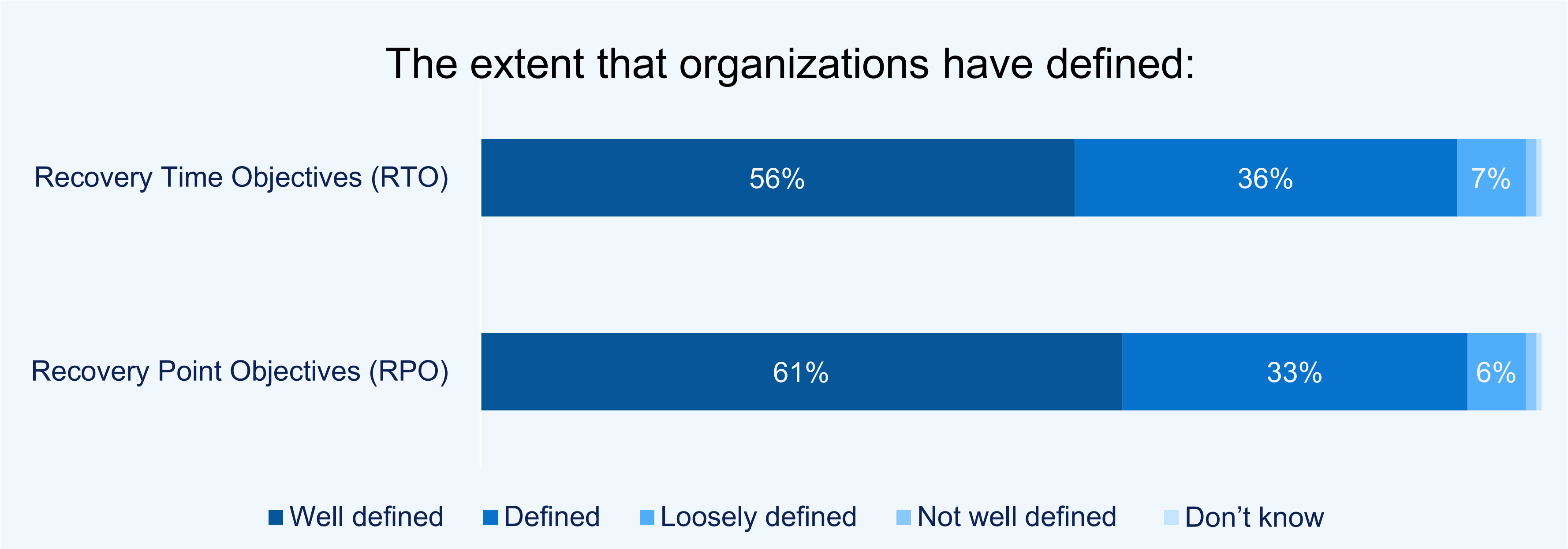
98%

Agree their organization needs to continually strengthen security as threats evolve

86%

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

The extent that organizations have defined:



Only 37% have **both areas** well defined

Of those with both well-defined RTO and RPO

73% have a mature cyber resilience strategy

Section 2: Secure

Preventing attacks and hardening the digital estate

DELL Technologies

Visibility Gaps and Protection Shortfalls

59%

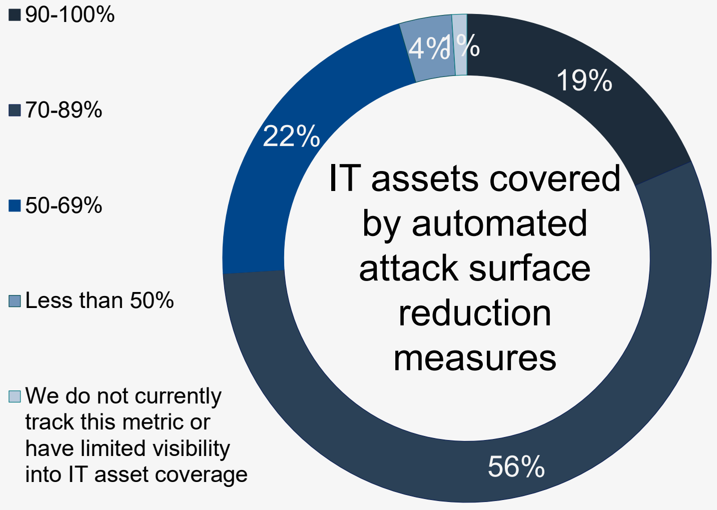
admit their backup data is not as well protected as it should be

45% 1,000-2,999 employees

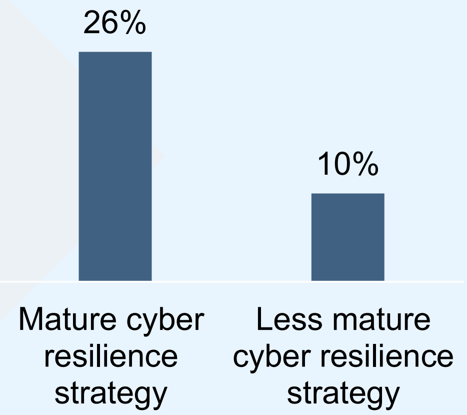
67% 3,000-4,999 employees

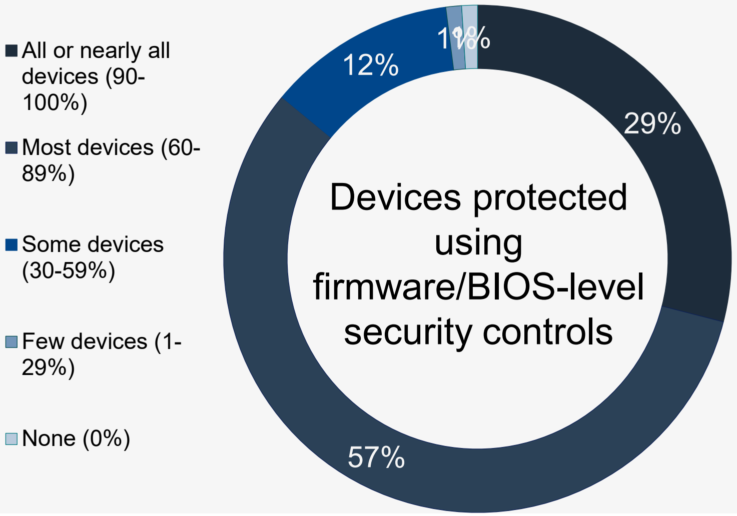
63% 5,000 or more employees

Continuous optimization does not eliminate coverage gaps, but it does give organizations a critical edge in resilience

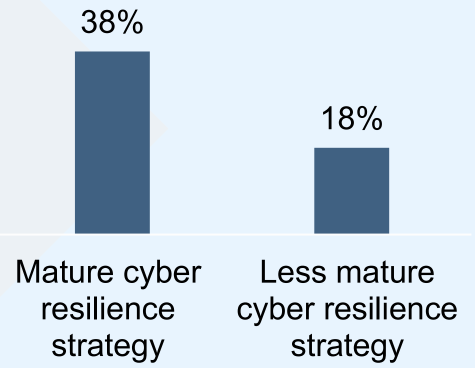


Organizations with 90-100% covered:





Organizations with all or nearly all (90-100%) covered:



From pre-deployment integrity to post-attack recovery: strengthen both ends of security

Processes/Methods used by organizations to ensure the integrity of IT hardware/software

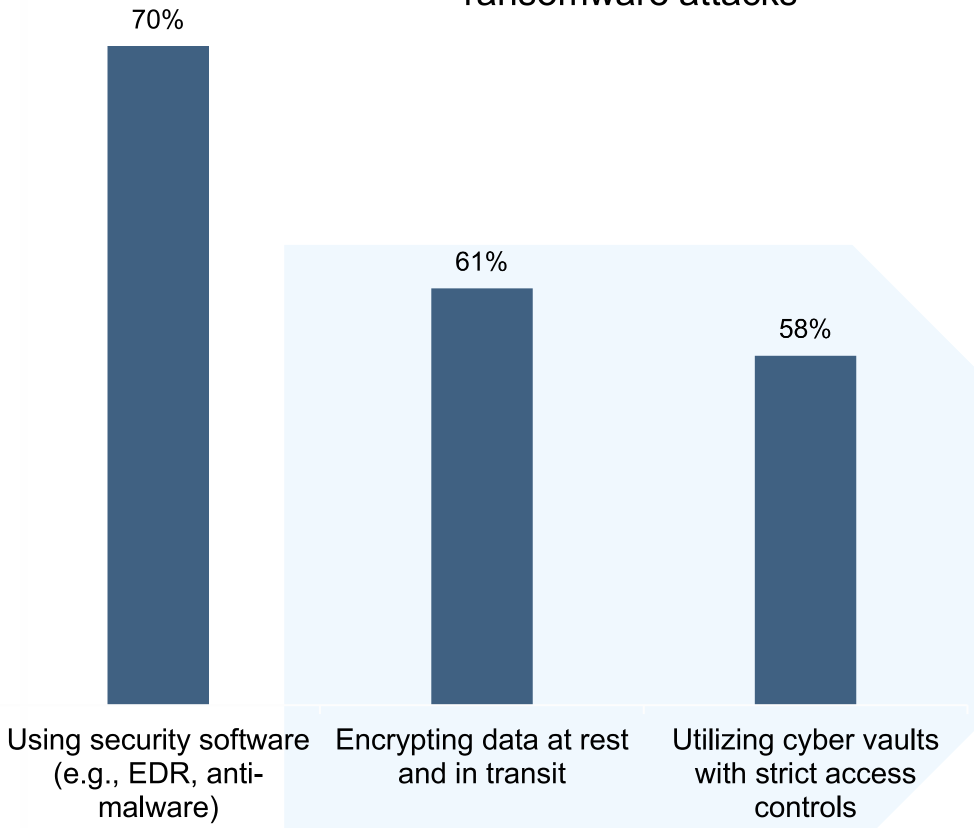
72%

rely on vendors for certifications and attestations and for systems with embedded tools that verify component integrity

70%

perform internal audits or manual reviews during staging/deployment

Methods used by organizations to secure critical data from ransomware attacks

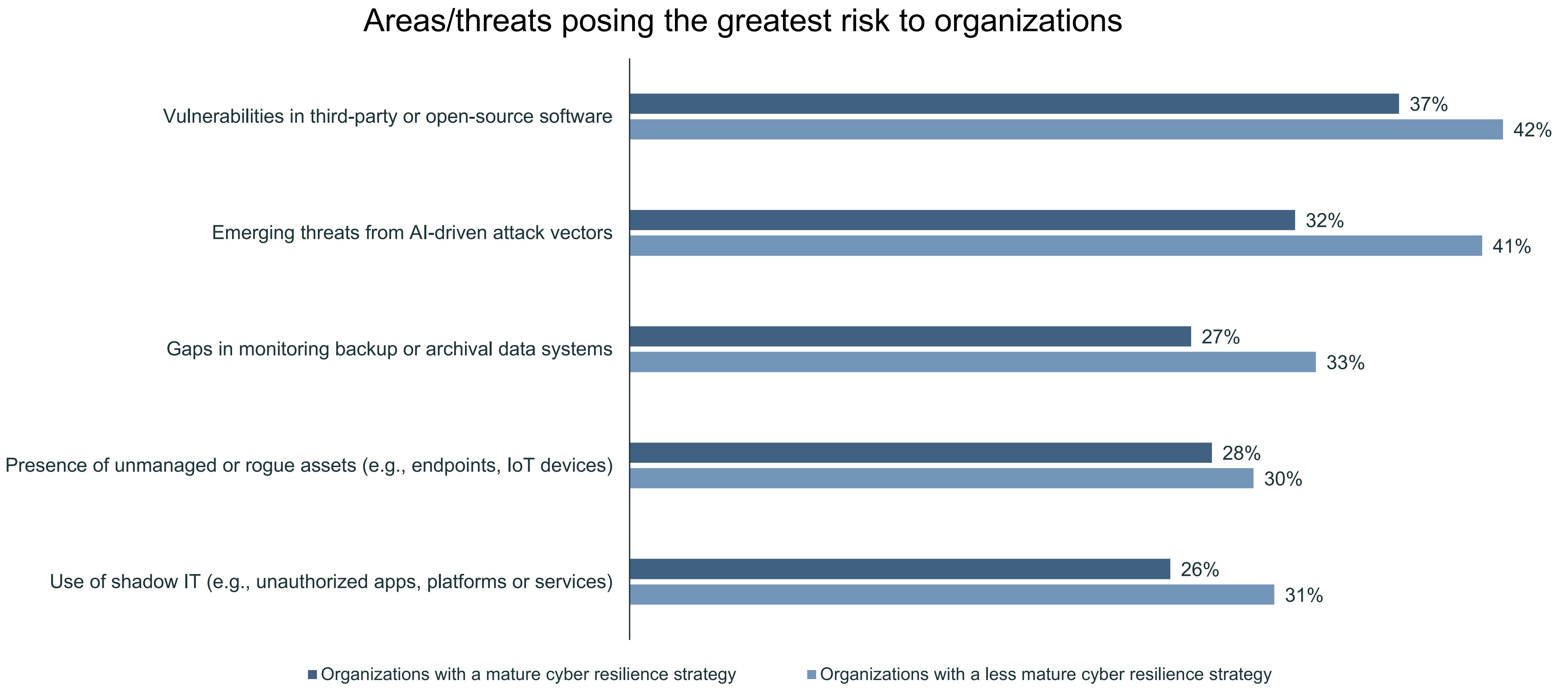


Organizations with mature resilience strategies more likely to use:

- **Data encryption (64% vs 55%)**
- **Cyber vaults (61% vs 56%)**

than organizations with less mature resilience strategies

Improving cyber resilience strategy may reduce risks faced



Section 3: Detect

Spotting and responding to threats before impact

DELLTechnologies

Utilizing AI and automation could uncover threats before they compromise backups

43% of organizations use AI/ML tools with proactive mitigation and response playbooks

Organizations with a mature cyber resilience strategy **3.2X more** likely to do this

62% of organizations use **AI/ML extensively to scan backup data** for indicators of compromise

Extensive use of AI/ML occurs **2X as often in organizations with a mature cyber resilience strategy**

84% believe threat actors are **increasingly attacking backups** during ransomware attacks

65% are **prioritizing investing** in automation and **AI/ML powered threat detection**

Incomplete visibility increases risk

59%

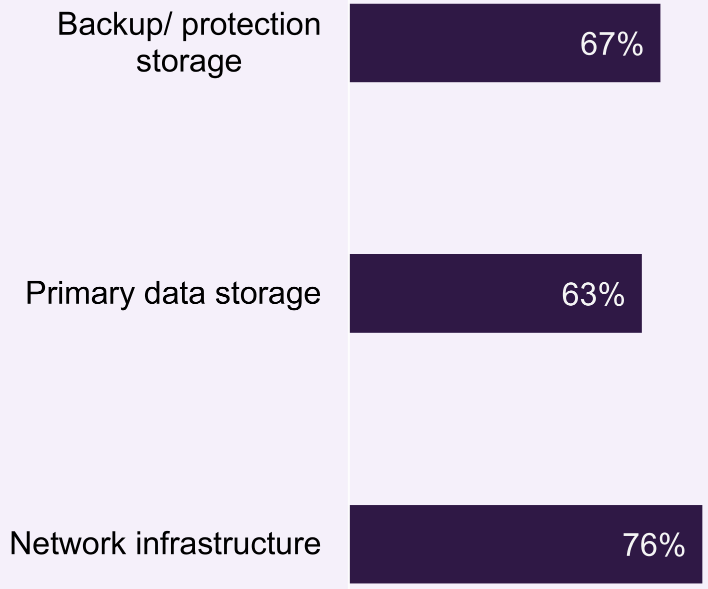
say they have high visibility into suspicious activity or compromised data within their backup systems

67% Organizations with a mature cyber resilience strategy

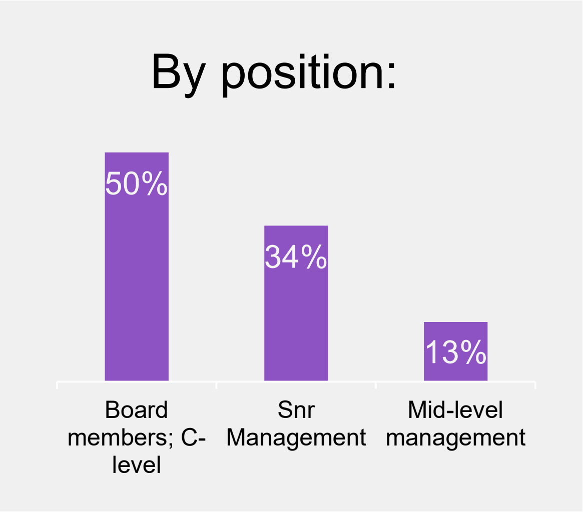
Vs

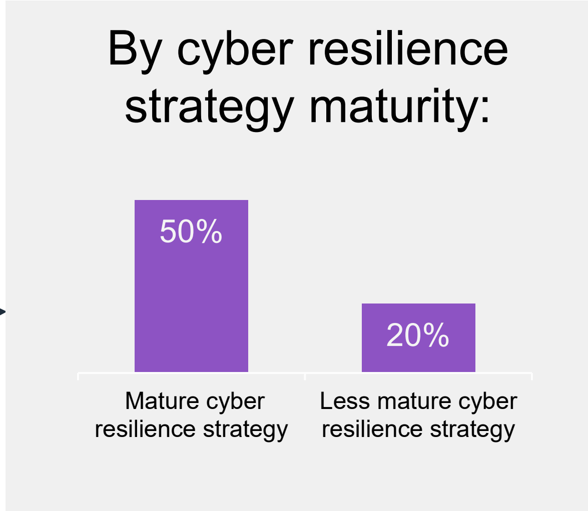
48% of organizations with a less mature cyber resilience strategy

Organizations with a robust platform for threat detection across the following areas



Only **36%** have a comprehensive platform **across all 3 areas**


By position:


By cyber resilience strategy maturity:

Section 4: Recover

Bouncing back fast, and within SLA expectations

State of recovery: many organizations meet targets, but continued improvement is essential to keep pace with the threat landscape

46% successfully **contained and recovered** with minimal impact

With **board members (58%)** more likely to state this than **mid-level managers (26%)**

58% of organizations **met their RTO/RPO targets**

⚠

By position: Board members (67%) Vs Mid-level management (51%)

#3 Primary driver of cybersecurity investment is a **recent cyber incident or near miss** at our organization

✓

58% are enhancing resilience capabilities to **meet regulatory or compliance requirements**

DELL Technologies

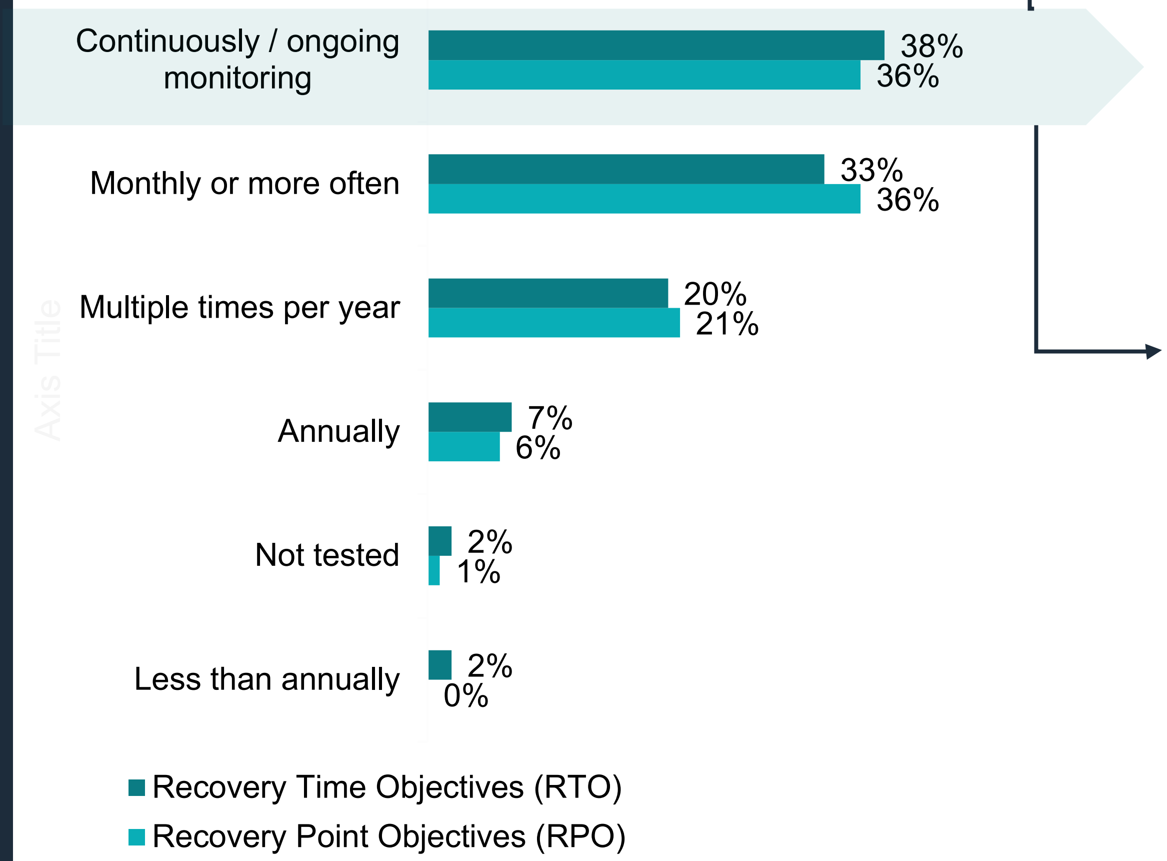
Frequent testing could improve recovery

> “Cyber resilience describes how my organization is ready to respond to and recover from any cyberattacks to ensure operational continuity…cyber resilience encompasses more strategies including data protection.”

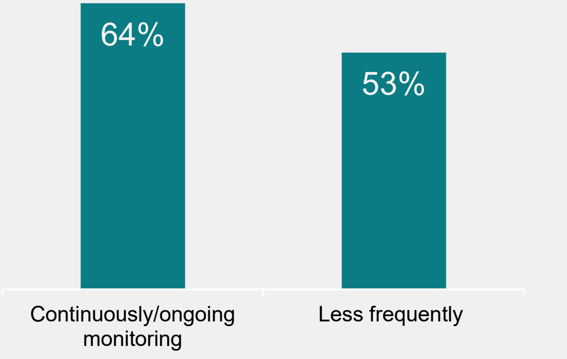
Snr Manager, Energy, Oil/Gas & Utilities

Testing is crucial to resilience, giving organizations a better chance to recover

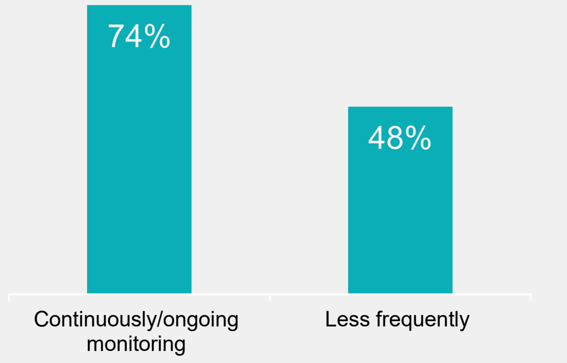
Frequency of testing RTO/RPO



Meeting RPO/RTO targets by testing: Recovery Time Objectives (RTO)



Meeting RPO/RTO targets by testing: Recovery Point Objectives (RPO)



Testing is fundamental to resilience

52%

Stated their organization's cybersecurity testing does not realistically simulate modern attack techniques

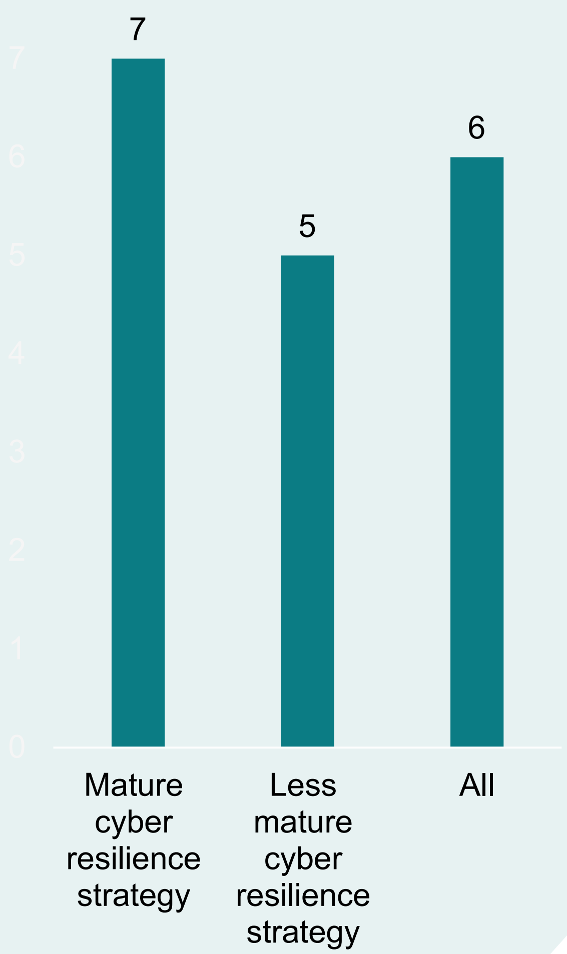
56% of board members; C-Level

Vs

67% Mid-level management

Regular practice is key to boosting recovery, but organizations should continuously plan for evolving threats

Average times per year organization conducts simulated cyberattacks



61%

of those who conducted simulated cyberattacks **monthly or more frequently successfully recovered** from a drill/cyber incident

38%

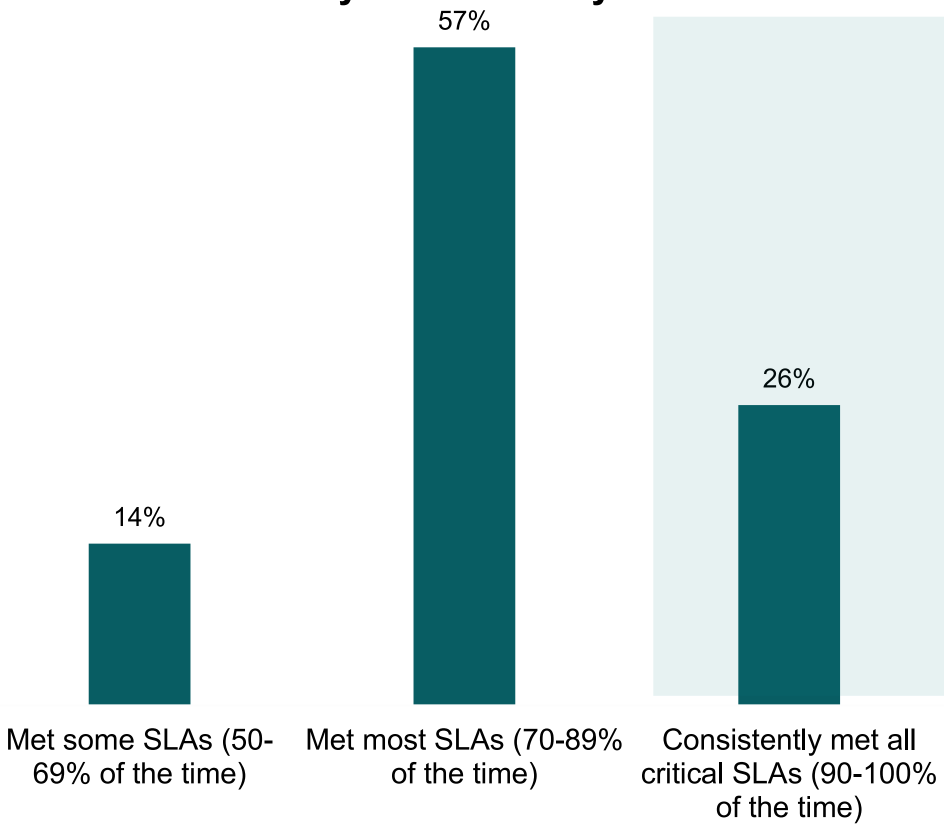
of those who conducted simulated cyberattacks **less than monthly successfully recovered** from a drill/cyber incident

> *Cyber resiliency is a greater priority during IT infrastructure planning to ensure we are down as little time as possible during a crisis.*
>
> Board Member, Energy, Oil/gas and Utilities

> *There's a difference between reactiveness and proactiveness. We try to be more proactive in our approach to cyber resilience.*
>
> Snr Manager, Manufacturing

SLAs are the proof point: organizations with mature strategies deliver on recovery promises

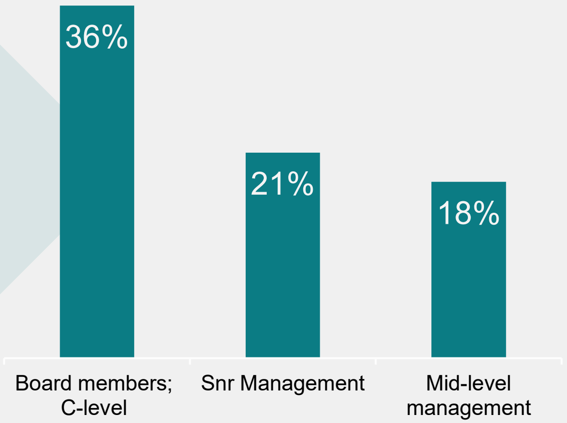
Frequency of organizations meeting SLAs for critical system recovery



2.3X

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

By position:



Section 5: Complexity, culture and what's next

Organizational barriers and future investment plans

Complexity, skills gaps, and overconfidence threaten cyber resilience, but AI and training could assist

Top challenges:

56%
Complex IT environment

44%
Vendor/ tool fragmentation

41%
Budget limitations

37%
Lack of skilled staff

Larger organizations more likely to face this:

60% 5,000 or more employees

55% 3,000-4,999 employees

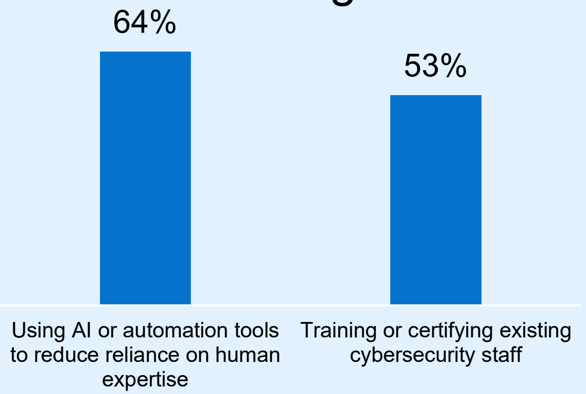
52% 1,000-2,999 employees

69%
think leadership overestimates their organization's readiness for a major cyber event

97%
Acknowledge they have shortfalls in their cybersecurity skills or expertise

BUT…

Organizations are acting through:



Looking ahead to investments

#1

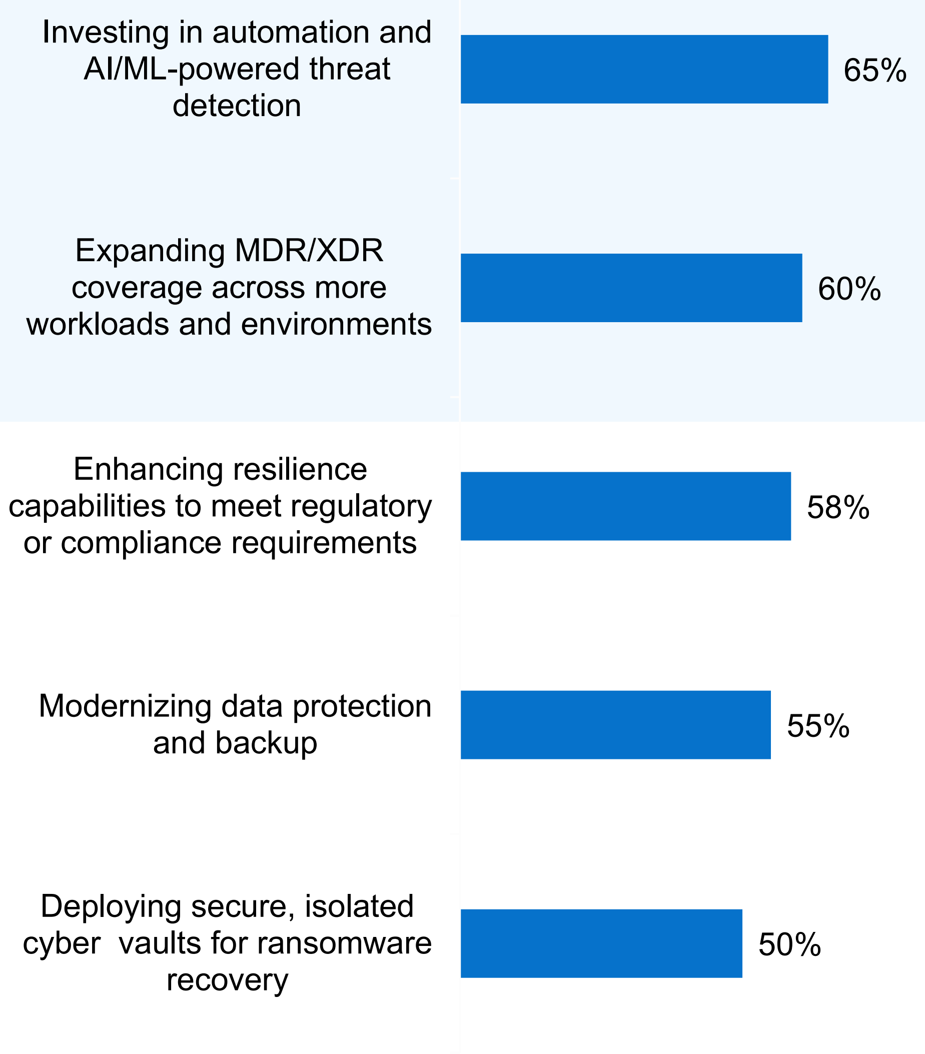
Driver of investment is the evolving threat landscape

98%

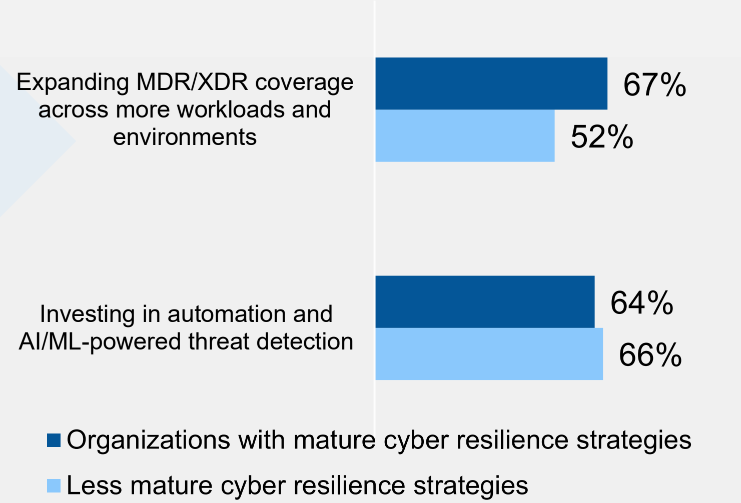
“My organization needs to continually strengthen its security as threats evolve”

To maintain a mature stance, continuous investment and optimization is the way forward

Prioritized cyber resilience investments over next 12 months



Mature cyber resilient organizations are continuously investing



Key takeaways

Key takeaways

54%

of organizations have a fully established and continuously optimized cyber resilience strategy

Continuously optimize resilience: Keep strengthening your ability to secure, detect, and recover to stay ahead of evolving threats.

59%

recognize their backup data is not as well protected as it should be

Enhance backup security: Use encryption, isolation, and immutability to keep backups safe from compromise.

Secure

36%

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

Adopt integrated detection: Link network, backup, and storage monitoring to deliver end-to-end visibility and close gaps across complex IT environments.

Detect

61%

of those who conducted simulated cyberattacks monthly or more frequently successfully recovered from a drill/cyber incident

Modernize and intensify testing: Use up-to-date attack simulations frequently while refreshing tactics regularly to reflect emerging threats.

Recover

69%

think leadership overestimates their organization’s readiness for a major cyber event

Foster a challenge culture: Encourage teams to question preparedness claims and surface potential weaknesses without blame.