

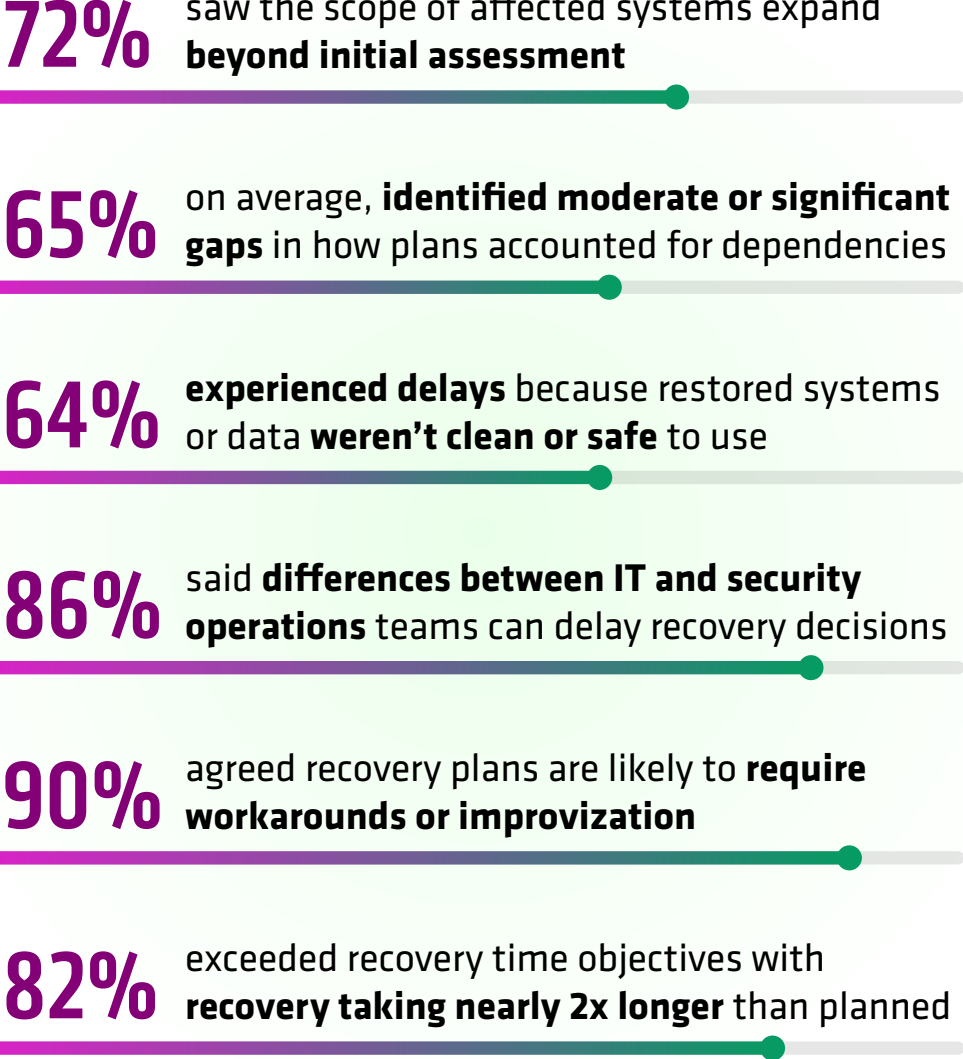
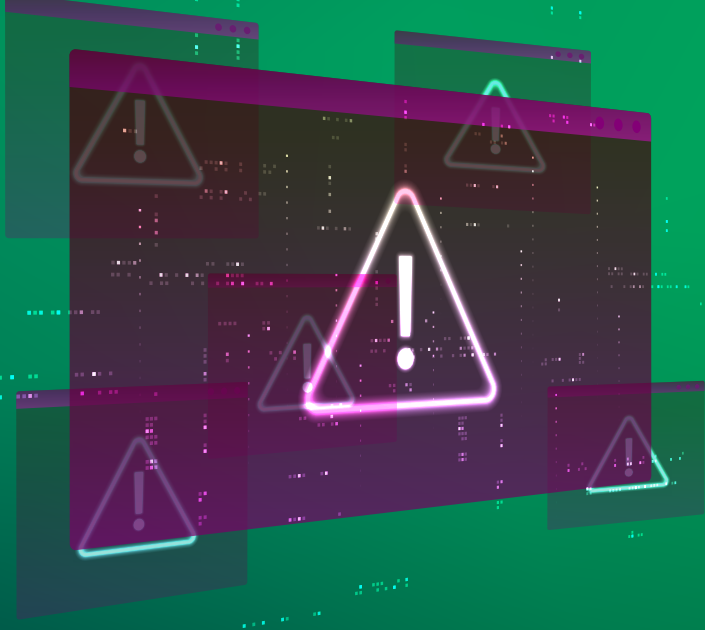
# CYBER RECOVERY PLANS WEREN'T DESIGNED FOR THIS MOMENT

*The world changed. Recovery plans haven't.*

A global survey of nearly 1,000 IT and security operations decision-makers from midsize organizations reveals what happens when plans built on long-standing assumptions collide with increasingly complex environments and the growing influence of AI.

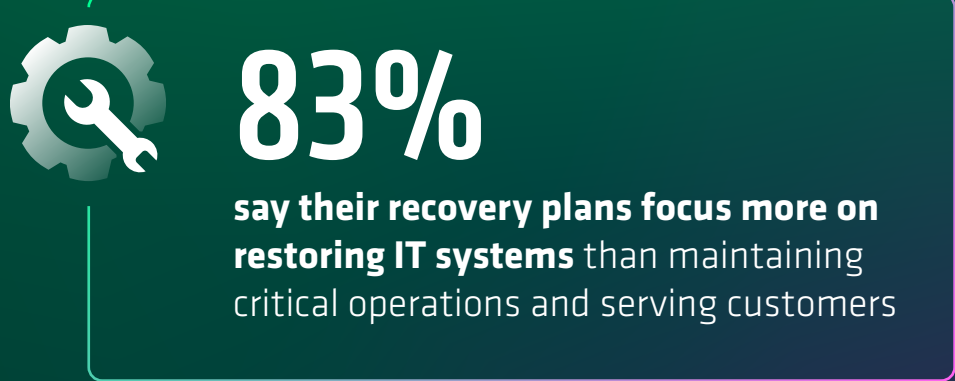
## WHERE RECOVERY PLANS FALL SHORT

Most recovery plans assume recovery will unfold in a predictable way. Midsize organizations that experienced a material cyberattack in the past 12 months often found otherwise.



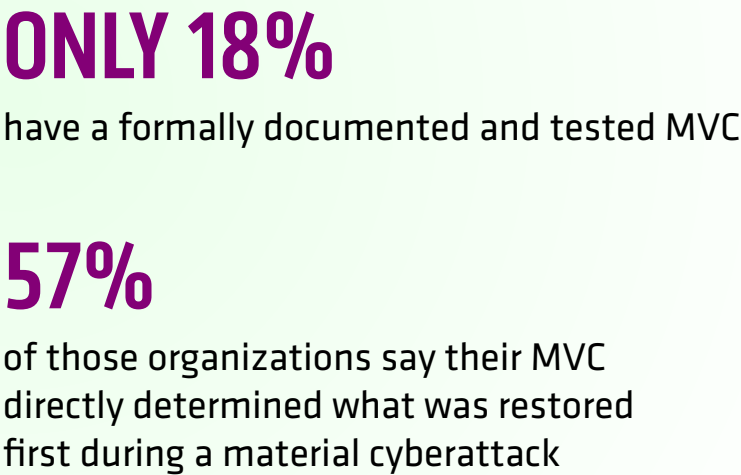
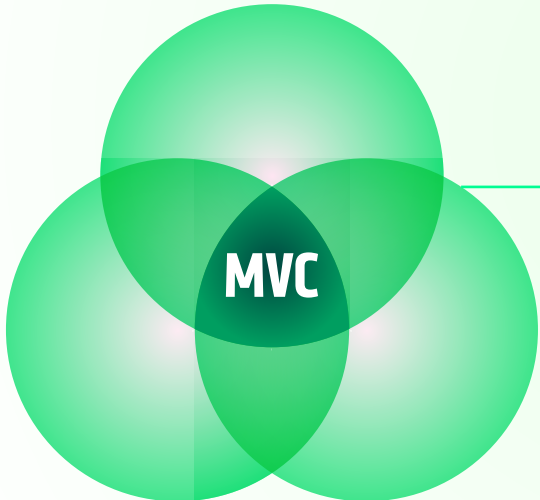
## WHAT MOST RECOVERY PLANS PRIORITIZE

Midsize organizations often make tradeoffs between recovery speed, system restoration, and business continuity.



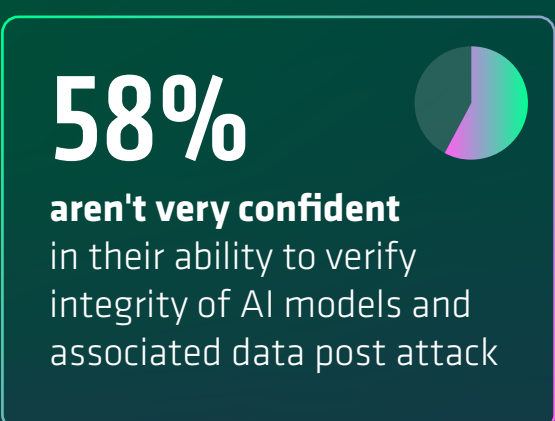
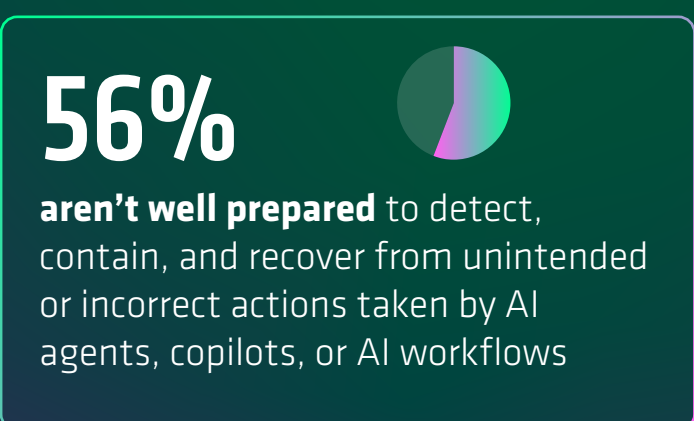
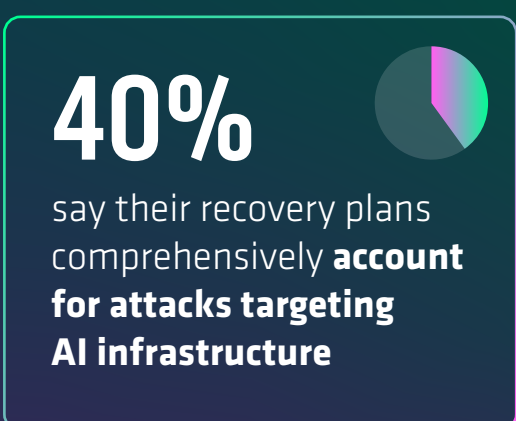
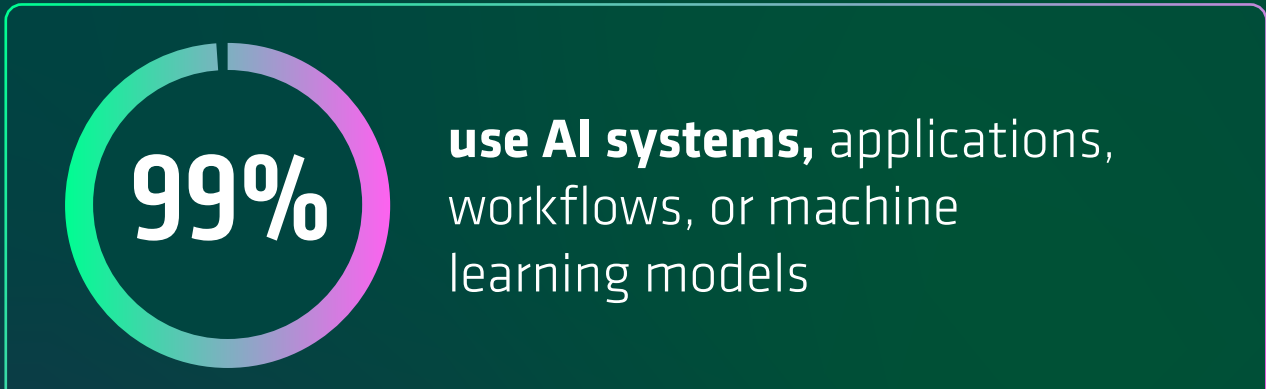
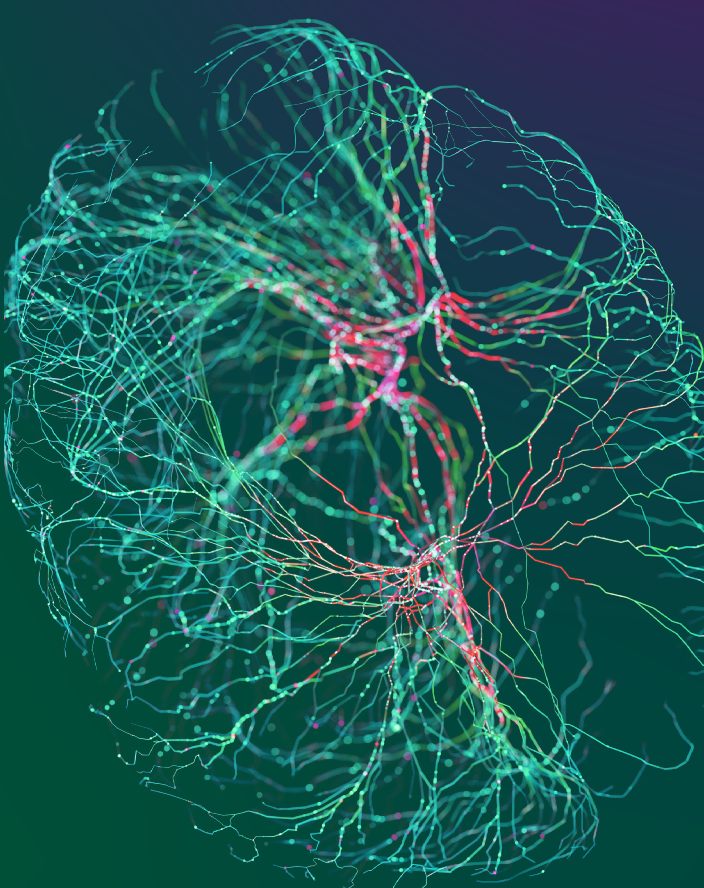
## FEW DEFINE WHAT MATTERS MOST BEFORE AN ATTACK

A Minimum Viable Company (MVC) helps midsize organizations prioritize and narrow the scope of recovery to minimize business disruption.



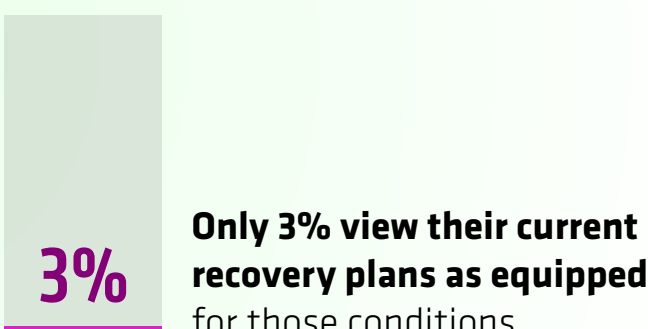
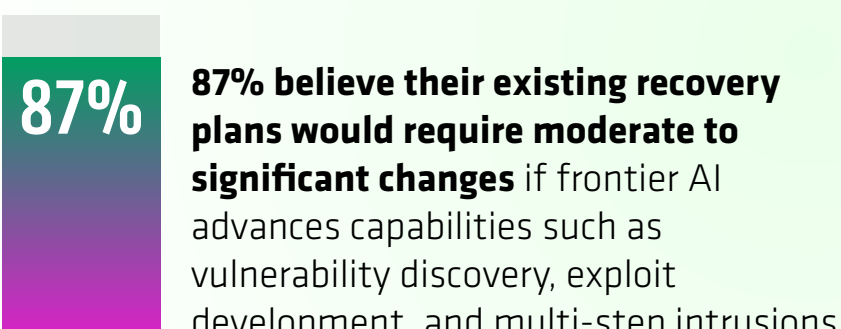
## AI IS BECOMING OPERATIONAL BEFORE IT BECOMES RECOVERABLE

As AI adoption accelerates, recovery planning is struggling to keep pace.



## CURRENT PLANS AREN'T BUILT FOR WHAT'S COMING

Midsize organizations expect frontier AI to place even greater pressure on today's recovery assumptions.



*Prepare for this moment. Plan for the next.*



Get more insights from the 2026 Cohesity Global Cyber Resilience Report





Download the Cohesity 5 Steps of Cyber Resilience® eBook





Explore Cohesity's cyber resilience solutions

