PUBLIC SECTOR CYBER RECOVERY PLANS WEREN'T DESIGNED FOR THIS MOMENT

The world changed. Recovery plans haven't.

A survey of more than 400 IT and security operations decision-makers from public sector 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. Public sector organizations that experienced a material cyberattack in the past 12 months often found otherwise.



74% saw the scope of affected systems expand **beyond initial assessment**

70% on average, **identified moderate or significant gaps** in how plans accounted for dependencies

69% **experienced delays** because restored systems or data **weren't clean or safe** to use

86% said **differences between IT and security operations** teams can delay recovery decisions

89% agreed recovery plans are likely to **require workarounds or improvisation**

71% exceeded recovery time objectives with **recovery taking nearly 2x longer** than planned

WHAT MOST RECOVERY PLANS PRIORITIZE

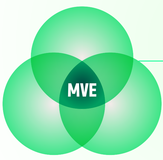
Public sector organizations often make tradeoffs between recovery speed, system restoration, and business continuity.

79% **prioritize speed of recovery,** even over certainty that restored systems were clean and safe

79% **say their recovery plans focus more on restoring IT systems** than maintaining critical operations and serving citizens

FEW DEFINE WHAT MATTERS MOST BEFORE AN ATTACK

A Minimum Viable Entity (MVE) helps public sector organizations prioritize and narrow the scope of recovery to minimize service disruption.

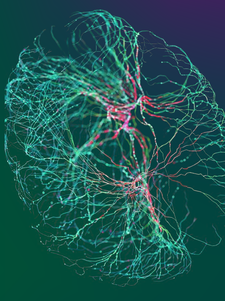


ONLY 14% have a formally documented and tested MVE

61% of those organizations say their MVE directly determined what was restored first during a material cyberattack

AI IS BECOMING OPERATIONAL BEFORE IT BECOMES RECOVERABLE

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



97% **use AI systems,** applications, workflows, or machine learning models

43% say their recovery plans comprehensively **account for attacks targeting AI infrastructure**

55% **aren't very confident** in their ability to verify integrity of AI models and associated data post attack

54% **aren't well prepared** to detect, contain, and recover from unintended or incorrect actions taken by AI agents, copilots, or AI workflows

CURRENT PLANS AREN'T BUILT FOR WHAT'S COMING

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

88% **88% believe their existing recovery plans would require moderate to significant changes** if frontier AI advances capabilities such as vulnerability discovery, exploit development, and multi-step intrusions

2% **Only 2% view their current recovery plans as equipped** for those conditions

Prepare for this moment. Plan for the next.

- Explore more insights from the 2026 Public Sector Cyber Resilience Report
- Book a Ransomware Resilience Workshop for Government Agencies
- Identify potential gaps in your resilience plan

METHODOLOGY

Cohesity commissioned Vanson Bourne to survey 3,200 IT and security decision-makers across 12 countries in July 2026. This included more than 400 participants from the public sector, representing organizations with 1,000 or more employees. For the purposes of this research, a material cyberattack was defined as having a measurable financial, reputation, operational and/or customer churn impact on their organization.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind. 6200055-001EN 9-2026