RISK-READY OR RISK-EXPOSED

COHESITY

The Cyber Resilience Divide in the Public Sector

Cyberattacks are no longer isolated events but an enduring feature of our digital world. Each day brings a new reminder as public sector organizations around the world are increasingly targeted. No organization is immune, and the growing frequency and sophistication of threats have led to a surge in material cyberattacks that cause measurable financial, operational, and reputational damage.

A GLOBAL SURVEY OF 399 IT AND SECURITY OPERATIONS DECISION MAKERS FROM PUBLIC SECTOR ORGANIZATIONS REVEALS THE REALITY.

67%
of organizations have faced a material cyberattack

49%
were hit in the past 12 months.

1 IN 4
have been attacked multiple times.

THE DAMAGE RUNS DEEP AND **COSTS ADD UP FAST.**

85% Lost revenue

42% Lost customers

61% Of publicly listed organizations had to review their financial guidance

97% Faced regulatory or legal consequences

92% Paid a ransom in the past 12 months

EVEN WITH THE EVIDENCE IN PLAIN SIGHT, MANY ORGANIZATIONS OVERESTIMATE THEIR RESILIENCE.

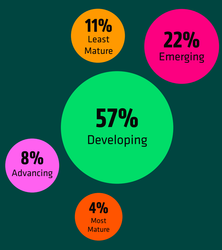
54%
have complete confidence in their cyber resilience strategy

MOST STILL PRIORITISE PREVENTION AND DETECTION OVER THE EQUALLY CRITICAL FUNCTIONS OF RESPONSE AND RECOVERY.

Order based on the NIST cybersecurity framework.
Box size shows highest to lowest proportion of cyber resilience investments.

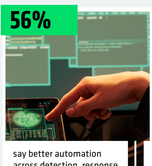
CONFIDENCE AND SPENDING PATTERNS **TELL ONLY PART OF THE STORY**

True resilience depends on the practices and capabilities that back them up. When assessed against real-world performance criteria, only 4% of organizations demonstrate maturity across five essential areas: **data protection, data recovery, threat detection and investigation, application resilience, and data risk optimization.**



An awareness of the need to enhance resiliency is driving the next evolution – powered by automation and AI. As threats become faster and more complex, automation is key to accelerating detection, streamlining response, and strengthening recovery.

56%



say better automation across detection, response, and recovery is one of the top lessons learned following the cyberattack

42%

believe AI will play a central role in how they detect and respond to threats including making some autonomous decisions

98%

plan to use AI to support data security operations by the end of 2026

ARE YOU RISK READY?

- **Download the cyber resilience public sector industry report** for detailed findings.
- **Book a Ransomware Resilience Workshop**
- Get our **"Five Steps to Cyber Resilience"** eBook to start advancing your maturity today.

Vanson Bourne surveyed 3,200 IT and security leaders from North American, Asia-Pacific, European and Latin American regions, representing organizations with 1,000 or more employees in 2025. Respondents included 399 participants from public sector organizations.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200040-001-EN 6-2026