



# Global public sector confidence in cyber resilience is misplaced

A new report from Zscaler, **Unlock the Resilience Factor: Why Resilient by Design is the Next Cyber Security Imperative**, highlights the need for greater prioritization and investment to ensure that cyber resilience strategies are prepared for inevitable future failure scenarios.

## KEY PUBLIC SECTOR FINDINGS

Against the backdrop of escalating threats and an increasingly volatile operating environment, business continuity is under attack

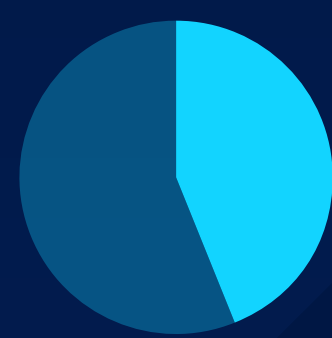
41%

of organizations experienced a **significant failure scenario** in the last 6 months

58%

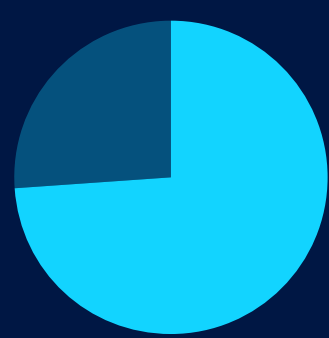
of organizations expect to experience a significant failure scenario within the **next 12 months**

### IT leaders feel well prepared for these kind of failure scenarios



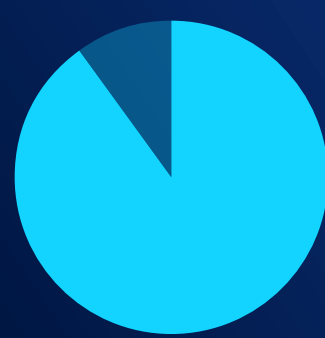
44%

of IT leaders believe their IT infrastructure is **highly resilient**



74%

label their organization's approach to cyber resilience as **mature**



90%

think their current cyber resilience measures are **effective**

### But more granular scrutiny uncovers inconsistencies, gaps and inefficiencies

ONLY

36%

of IT leaders say their cyber resilience strategy is **up to date** in response to AI's rise

40%

admit to **not having reviewed** their cyber resilience strategy in the last 6 months

### Less than half of organizations are using each of the following proactive security tools



RISK HUNTING

40%



ZERO TRUST MICRO-SEGMENTATION

37%



DECEPTION TECHNOLOGIES

29%

### Lack of leadership investment identified as a friction point



ONLY 33%

of IT leaders believe cyber resilience is a top priority for leadership



54%

agree that the budget assigned to cyber resilience doesn't meet the escalating need



ONLY 33%

say the cyber resilience strategy is included within their organization's overall resilience strategy



ONLY 39%

say the CISO is involved in resilience planning

A mindset shift is required to overcome the key barriers to implementing a robust cyber resilience strategy

60% of IT leaders believe their organization overly prioritizes prevention in its cyber security strategy

63% say their leadership continues to define cyber security failure as initial access (by a threat actor)

The top three barriers to becoming more resilient:

40%

COMPLEXITY OF IT/SECURITY INFRASTRUCTURE

32%

A LACK OF RESOURCES AND SKILLS

30%

LACK OF INVESTMENT

### Building cyber resilience into the business strategy from the start

IT leaders can see the correlation between a robust cyber resilience strategy and stronger business performance, but are struggling to achieve results from current efforts.

57%

are seeing a **reduction** in data loss

55%

are experiencing **faster** incident recovery

50%

report **faster** incident detection and containment

Today's business context demands that public sector organizations pay more attention to cyber resilience — that they better fund it, more frequently review it, and increase their expectations of it. A fundamental shift in approach and mindset is needed to make cyber resilience a vital part of the security strategy from the start. We call this becoming **'Resilient by Design'**.

Learn more about pursuing a **'Resilient by Design'** approach, enabled by the Zero Trust Exchange platform, [here](#). [Read the report](#)

## METHODOLOGY

In December 2024, Zscaler commissioned Sapio Research to conduct a survey of 1,700 IT decision-makers (IT leaders) across 12 markets (Australia, France, Germany, India, Italy, Japan, Netherlands, Singapore, Spain, Sweden, UK & Ireland, US). 206 of these IT leaders work at companies within the public sector industry.

## ABOUT ZSCALER

Zscaler accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.