THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

The New Imperative: Test Before You're Tested

Fady Richmany warns that traditional data-protection measures are insufficient. Organizations must prove they can recover before a breach strikes.

CONTROL FRAMEWORK

Data Protection vs. Cyber Resilience

Data protection secures information at rest and in transit. Cyber resilience adds the ability to continue operations and restore services after an incident.

→ Protection: encryption, access controls, monitoring

→ Resilience: incident response, recovery validation, adaptive processes

CONTROL FRAMEWORK

Why Un-Tested Recovery Is a Hidden Risk

Recovery plans that have never been exercised often contain gaps that surface only during a real attack, leading to extended downtime and revenue loss.

→ Assumptions remain unchecked

→ Dependencies may be unknown

→ Stakeholder roles can be unclear

CONTROL FRAMEWORK

Practical Testing Methods

Select the right test for your maturity level and risk appetite.

→ Tabletop exercises – scenario discussion without systems

→ Red-team simulations – adversary-style attacks on recovery processes

→ Automated failover drills – scheduled, technology-driven restores

CONTROL FRAMEWORK

Include Testing as a Core Governance Practice

Make recovery validation a regular agenda item for risk committees, audit cycles, and compliance frameworks.

→ Set a recurring test schedule in the risk register

→ Document findings and use them to update policies

→ Share results with leadership alongside security metrics

CONTROL FRAMEWORK

Cross-Functional Collaboration Is Critical

CIOs, CISOs, and business unit leaders must co-own recovery objectives, share ownership of test outcomes, and align on remediation priorities.

→ Joint ownership of recovery service level objectives

→ Shared responsibility for test planning and execution

→ Unified communication plan for post-test findings

EXECUTIVE TAKEAWAY

Executive Takeaway

Validated recovery testing converts static data protection into active cyber resilience, ensuring the organization can sustain operations when attackers strike.