PRESIDIO®

WORKSHOP

Cyber Resilience Workshop & Roadmap

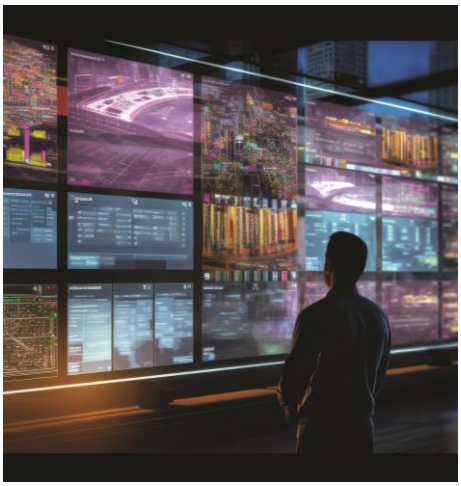
Ransomware has evolved into a three-stage extortion model: infiltrate, exfiltrate, and extort. This half-day to full-day workshop, delivered jointly by Presidio's Cyber Security and Modern Platforms teams, assesses your posture, educates your team on the real threat landscape, and builds a practical roadmap to resilience.

Who Should Participate

Ideal for organizations with aging backup infrastructure, limited cyber resilience testing, or seeking to align data protection and security programs before a threat occurs.

Recommended Attendees:

- CISOs, CIOs & IT Directors seeking executive alignment on cyber risk
- Infrastructure & Storage Teams evaluating immutability and vault solutions
- Security Operations Teams looking to strengthen IR readiness
- Compliance & Risk Officers needing to validate recovery SLAs
- Organizations that have never tested a ransomware recovery scenario



Workshop Topics

The following topics may be covered during the workshop:

- Current ransomware threat landscape & real-world attack case studies
- How modern attacks bypass traditional backup strategies
- Data Security Posture Management (DSPM) fundamentals
- The 3-2-1-1-0 backup rule & immutable vault architecture
- Incident response using the PICERL model
- MDR, EDR, and XDR defense layers explained
- Data exfiltration prevention strategies

Key Workshop Outputs

Gain immediate value and insight through the following key outputs of the workshop:

- Facilitated Workshop Deck covering ransomware landscape, DSPM, 3-2-1-1-0 rule, and PICERL model
- Cyber Resilience Readiness Summary across Identify, Protect, Detect, Respond, and Recover
- Gap analysis identifying critical vulnerabilities in current posture
- Personalized next-step recommendations and 4-phase resilience roadmap

Benefits of Workshop

The workshop provides your leadership team with the following benefits:

- Dual-team expertise: Unifies Cyber Security and Modern Platforms Data Protection in a single engagement
- Real-world threat intelligence from Presidio's MDR and Threat Strike Team
- Vendor-neutral architecture: Rubrik, Cohesity, Dell, Veeam, Commvault, Veritas — we recommend what fits
- Tested methodology: Recovery test workflows, realistic scenarios, and PICERL-aligned runbooks
- Regulatory alignment: Supports NIST CSF 2.0, Sheltered Harbor, and cyber insurance requirements

Contact Presidio today:
www.presidio.com/contact-us