

Cybersecurity

Ransomware Readiness Assessment



THE CHALLENGE

Ransomware has become the top cybersecurity threat for many organizations, across all sizes and industries. Many are uncertain as to the resilience of their environment against the threat posed by the current generation of ransomware. They are not sure about their ability to respond to a ransomware incident and might not even be sure as to what a ransomware response would entail.

THE SOLUTION

Most organizations know that the primary threat posed by ransomware is the encryption of data, effectively denying access to that data. Modern attackers may also exfiltrate data prior to encrypting it, adding the second threat of a data breach or extortion to the equation. Presidio proposes the Ransomware Readiness Assessment to establish confidence about your cybersecurity position as it relates to ransomware.

Ransomware Readiness Assessment – Presidio will identify security vulnerabilities within the IT environment that may be exploited to by an attacker to propagate ransomware throughout the organization to encrypt data. This includes a review of:

- ◆ Information system security design, architecture, and controls
- ◆ Wireless network and mobile device security
- ◆ System maintenance procedures
- ◆ Security review of key applications
- ◆ System and service enumeration
- ◆ Vulnerability identification

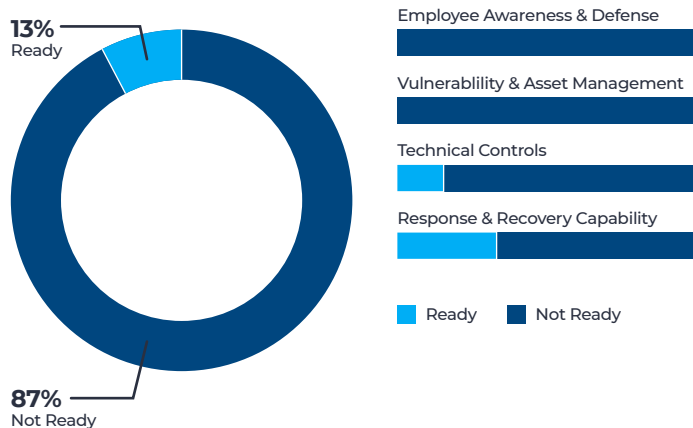
Ransomware Attack Simulation – Presidio will perform a simulated ransomware attack against the client environment. The attack will be initiated through a phishing campaign to deliver a simulated ransomware agent. The agent will move through the client environment using the same techniques employed by real malware, mapping the environment as it spreads. Data gained through this simulation will be used to identify gaps that need to be addressed as well as identify what data would be encrypted by real ransomware.

Ransomware Incident Response Review – Presidio will review the client’s current Incident Response Plan, as well as current backup and recovery capabilities. This assessment is key to identifying how well prepared the client is to respond to an actual ransomware attack.

The Assessment will identify key areas of readiness including:

- ◆ Employee Awareness
- ◆ Vulnerability
- ◆ Technical Controls
- ◆ Response & Recovery

READINESS BY CATEGORY



Ransomware Readiness Assessment

Along with identifying a client's specific gaps, this assessment will show how you compare to other similar companies. In addition, the report provides an initial assessment of the potential annual financial risk, based on the current Ransomware readiness profile.

The Ransomware Readiness Assessment is quick to execute (typically <3 weeks) and provides comprehensive and immediately actionable results.

KEY BENEFITS

Presidio helps our clients to protect, prepare for, defend against, and recover from successful ransomware cyber-attacks by providing the visibility they need to identify and mitigate their risks. We help them become Ransomware Ready.

Many clients do not have a detailed plan of how to react in a real-world situation of a ransomware attack. Some clients will have implemented new systems, but do not yet have the confidence that those solutions are providing the security posture that they desire.

Our goals are to improve the client's resilience to the ransomware threat and lay the foundation to effectively manage incidents by limiting impact to the business, reducing time and cost of recovery, and minimizing collateral damage such as brand reputation.

WHAT MAKES US DIFFERENT

Presidio is a trusted partner to our clients, securing their infrastructure, employees, clients and assets from ever-growing cyber threats. Our clients trust Presidio:

- ◆ **Deep Cyber Experience** – Presidio's highly-credentialed cybersecurity consultants collectively have decades of combined practical experience spanning cyber security governance, architecture, and operations
- ◆ **Real Systems Intelligence** – The Ransomware Simulation component of the assessment utilizes an agent that closely emulates the capabilities of modern ransomware. This provides an unparalleled view into the actual vulnerabilities and potential impact a ransomware attack represents to the organization



WHY PRESIDIO

Presidio is a leading digital systems integrator, with deep experience in networking, cloud computing and broad hybrid infrastructures. Presidio recognizes that cybersecurity is foundational to the success of any business and has a highly specialized expert team at the ready. Our clients benefit from:

- ◆ Services methodology built on recognized industry standards including NIST, CIS, and ISO
- ◆ Compliance depth & breadth including PCI, HIPAA, NERC CIP, GDPR, CCPA, SOC 2, ISO 27001, DFARS 800-171, CMMC
- ◆ Multi-discipline experts provide for a broad view of client's potential vulnerabilities
- ◆ Deep cybersecurity services bench and broad security services solutions provide domain expertise and consistent deliverables

Presidio Cybersecurity Practice covers a broad security services portfolio. Our highly skilled and tenured cybersecurity practitioners maintain leading industry certifications, provide thought leadership and practical industry experience. We have conducted thousands of engagements across all major industry segments. Getting started with Presidio is easy. Let's explore how we can secure your business.

Contact Presidio today: www.presidio.com