

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



