CYBERSECURITY

Ransomware Assessments

Ransomware attacks continue to rise at an alarming rate and each one poses a unique risk; Quest helps you combat these threats with our comprehensive Ransomware Assessments. Our assessments are focused solely on ransomware rather than natural disaster threats. The following are the areas we review for the assessments:

Data Analysis

- Review logs for firewall for the past 30 days for source and destination origins.
- Review IDS/firepower logs including FW.
- Review firewall configs for stale ACLs or liberally open ACLs.
- Review configuration logs for 0365 (hardening, enable multi-factor authentication, limit external forwarding, minimize access methods, enable audit logging, leverage scripts, utilize secure score, etc.).

Learn more about Quest's **Cybersecurity services.**

- Review device logs for the past 30 days (all log data going into a SIEM).
- Review AV logs for past 30 days.
- Review external IP address information (ASN # would work here) and all DNS domains associated with Client that are tied to email.
- Review last cybersecurity executive presentation/report.
- Execute Quest Packaged Scripts (QPS): golden ticket, AD domain scripts, and O365 security scripts.
- Review current patch report.
- Review/run reputation report.
- Review SAN capability of SAN level snapshots.
- Determine quantity, frequency, and whether they are configured.
- Last penetration test/vulnerability scan report (on all Internet IP range).
- Review backup report (RTO/RPO) and DR capability.
- Also review Immutable vs AirGap, 3, 2, 1, 0.

Review Controls

- Review security monitoring practices (tools and processes).
- Backup and AD servers for access control.
- Review inbound and outbound ACL filter capabilities.

- Review third-party VPN controls.
- Review DLP controls (Endpoint Encryption); specifically looking for lost/stolen protection.
- Review Change Control practices (how changes are made, tested, tracked, confirmed, etc.).
- Review Edge capabilities for geo-blocking.
- Review Edge and ISP capabilities for RDOS controls.
- Review endpoint protection controls and distribution.
- Review O365 access control and authentication.
- Review email flow and security (DKIM, DMARC, anti-malware, URL defense, encryption, etc.).
- Review Access Control overall (especially AD accounts used for Management) and MFA for Management as well as access and identity management.
- Review third-party application (Mobil vendor) controls for SDLC current and future.
- Review asset management and controls.
- Review mobile solution (VMware/Vox).
- Review AWS IAMs controls.
- Physical security controls (facility and data).
- Review wire transfer controls (between CFO and CEO/staff)/invoice security.
- Review last risk assessment (including B2B/third-party service providers).
- Review the last cybersecurity training performed by all personnel (this is different from phishing tests).
- Review travel security training (how to stay safe while traveling).
- Review past 60 days' phishing test and controls.
- Review process, frequency, and validity of user testing.

Recovery Capabilities (With Scenarios)

- Review written Incident Response Plan according to regs.
- Review capabilities to recover from a ransomware or ransom DOS (RDOS) attack.
- Review risk with cross-contamination with third-party vendors.

Analysis

- Discuss data gathered.
- Discuss controls that were reviewed.
- Document findings with gaps and recommendations.

Deliverables to be Provided as Part of This Statement of Work:

- Written report of findings and recommendations
- Design for survivability

The Following Areas of Concern Can Be an Add-On to the Base Scope:

- Application Code Review
- API code and standards review
- 3rd Party application/service validation