CYBER MITIGATION CASE STUDY

Cyber Risk Assessment Uncovers 5000 Vulnerabilities: 50 Percent Exploitable

Critical Business Challenges

Our client is a retail organization who was concerned with the amount of ransomware attacks targeting the SMB market segment and the retail industry. Quess GTS was asked to perform a Cyber risk assessment which combined deployment of intelligent agents to inspect the environment, interview with key staff and a site visit to key locations.

Our Solution

Quess GTS partnered with the customer to install non-intrusive intelligent agents throughout the environment, reviewed Cyber hygiene policies and practices, third party vendor risk policies and process around release management, patching, backup and recovery, business continuity and data management. Information was synthesized from the various sources and presented back to the executive, technical and operations team.

The Outcome

- Five thousand plus vulnerabilities found due to end of life, end of support and version management.
- Fifty percent of vulnerabilities were identified as exploitable from industry Cyber intrusions.
- Backup and recovery processes needed enhancements.
- Cyber awareness training for the Human Firewall was not in place.
- Third Party Vendor Risk Mitigation was not in place.
- Recommendations were organized into an integrated roadmap with short, medium, and longer-term initiatives scoped.
- Mitigation activities are currently being implemented with Quess as their partner.

Results

- Enterprise Risk Profile Communicated
- Cyber Awareness Culture Developed
- Vulnerability Management and Pen testing Mitigated Risks
- Incident Response and Business Continuity Plans Outlined