Bonum ADVISORY

Cybersecurity

Cybersecurity risks threaten business continuity, stakeholder trust, and competitive advantage. Yet many organizations lack visibility into their actual security posture. Effective cybersecurity requires strategic assessment, prioritized remediation, and ongoing readiness. Partnering with us to evaluate your infrastructure, applications, and data protection will help you understand your risks, allocate resources efficiently, and build defenses that protect what matters most.

Risk Assessment

Assess infrastructure security, identify vulnerabilities and critical assets, and deliver prioritized risk matrix high-lighting immediate remediation needs.

Security Posture Review

Evaluate current state of security controls, policies, and processes against industry frameworks (NIST, CSF, ISO 27001) to identify gaps.

Vulnerability Assessment

Conduct technical scanning and ethical hacking to uncover exploitable systems, networks, and applications before attackers find them.

Security Awareness

Assess vendor and supplier security practices, evaluate supply chain vulnerabilities, and establish ongoing monitoring protocols.

Incident Response Readiness

Develop or review incident response plans, conduct exercises, and ensure teams are prepared to detect, contain, and recover from breaches.

Compliance Assessment

Evaluate adherence to applicable regulations (SOC 2, HIPAA, PCI-DSS, GDPR) and develop remediation roadmaps for compliance gaps.

Third-Party Risk Management

Design and implement training programs, conduct phishing simulations, and measure organizational security culture and employee readiness.

Threat Modeling & Analysis

Identify potential attack vectors, threat actors, and attack scenarios specific to the client's industry, assets, and business model.

info@bonumadvisory.com (310) 857-0412 www.bonumadvisory.com