TREXIN CASE STUDY

MITIGATING THIRD-PARTY CYBER RISKS

Trexin conducted a comprehensive risk assessment of a health insurance subsidiary's cybersecurity controls and resilience strategies.

BUSINESS DRIVER

The rising threat of a third-party risk has become a growing concern among CISOs. Third parties, ranging from external vendors and partners to closely held subsidiaries operating semi-independently from their parent organization, can present security risks. In one well-known example, a major breach at a healthcare payer resulted in $3B in direct costs and business disruptions. In response, the CISO of a multistate health insurance payer approached Trexin to assess its subsidiaries, focusing on security controls, risk management, and resilience. This project assessed the subsidiary in a "friendly assessment", going beyond documenting risk to helping mitigate risks. Trexin's cybersecurity expertise and established relationships fostered collaboration between all parties, navigating a complex engagement effectively.

APPROACH

Trexin's approach combined multiple frameworks into a single, seamless assessment. It leveraged Trexin's DEADONS+1 methodology, Information Systems Audit and Control Association's (ISACA) Capability Maturity Model Integration (CMMI), National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), People-Process-Technology categorization, a penetration test, and the Client's own methodology. Critical elements evaluated included data security, system configurations, user access, and network integrity. Penetration testing and vulnerability scanning identified weak points such as open ports, unpatched software, and configuration flaws. Throughout the assessment, Trexin conducted interviews with key IT executives to evaluate existing processes, documentation, and system configurations. Documentation provided by the subsidiary was reviewed for completeness and potential gaps. This comprehensive approach ensured a thorough understanding of the subsidiary's security posture, highlighting the key risks and areas for improvement.

RESULTS

Each maturity area was assessed and given a current, future, and projected CMMI score for one year post-assessment. Risks were categorized as high, medium, and low security levels, with 6,000 vulnerabilities, of which 3,000 were classified as high. Of these, 87% of the identified risks can be mitigated by prioritizing critical risks during the Azure migration. Each risk category included recommendations for mitigation and its impact. Identified risks and their expected resolution timelines were used to create a maturity enhancement roadmap, spanning 12+ months, with each phase highlighting progress and impacted areas. The final deliverables summarized the current state, progress made, and a framework for continuous improvement, ensuring a secure security position. This process also provided confidence that subsidiary risks are well-understood, even if not fully mitigated, reinforcing a clearer risk landscape for future decision making.

CONTACT US

Healthcare Practice
hc@trexin.com
www.trexin.com

TREXIN
TRUST • EXPERIENCE • INNOVATION