CASE STUDY

FINANCIAL SERVICES FIRM **BEEFS UP CYBERSECURITY PROGRAM AHEAD OF SEC SCRUTINY**

RESULTS AT A GLANCE

- Financial services firm recognized vulnerability to increasing cyber threats.
- Gap analysis considered five control stages and 96 subcategories.
- Provided 80 recommendations used to set goals and provide funding.

CLIENT CHALLENGE

Senior management at this mature financial services firm recognized that it is vulnerable to increasingly common and complex cyber threats. While the firm had a skilled and experienced technology team, management also recognized that additional security controls were needed to achieve parity with its peer group. When the company received notice from the SEC foreshadowing increased regulatory scrutiny, management knew it needed an objective, third-party assessment of controls maturity and prioritized list of remediation projects so it could make wise investment decisions.

APPROACH

Management engaged Coalfire to serve as an independent assessor organization, and instructed Coalfire to conduct a gap analysis that would compare the firm's current controls program to the standards put forth in the NIST Cybersecurity Framework, v1.0. Management also asked Coalfire to develop a corrective action plan for significant control deficiencies.

EXECUTION

Over a six-month period, Coalfire conducted an assessment that consisted of technical testing, document review, observation and inspection. The assessment considered all five control stages in the NIST CSF (Identify, Protect, Detect, Respond, Recover) and each of the 96 subcategories, mapping that framework to the guidelines provided by the SEC. Coalfire met with personnel, gathered evidence and walked through the environment to determine what The Firm's documented policies were to support its findings and provided recommendations for each observed gap. From there, Coalfire reviewed the systems currently in place to whether they are following their stated process and procedures.

RESULTS

Coalfire's report provided senior management with an accurate, reliable and defensible assessment of the company's current cybersecurity program. In addition, Coalfire provided more than 80 discrete recommendations. Based on these recommendations, senior management was able to set meaningful goals and provide adequate funding to the firm's information security officer. The firm now has a clear path to a more mature cybersecurity management model and conducts annual re-assessments to measure its progress in reducing cybersecurity risk. A Coalfire-led validation process will become an annual part of the checks and balances and to track their increased performance.

COALFIRE

North America | Latin America | EMEA
877.224.8077 | info@coalfire.com | coalfire.com

Follow us to get the latest updates:

CS_CyberRiskFinancial_05252016