

INVESTMENT FIRM ANTICIPATES HEIGHTENED REGULATORY SCRUTINY

AT A GLANCE

Regulatory agencies are increasing their focus on cybersecurity.

Comprehensive gap analysis considered five security functions and 96 subcategories.

Risk and controls assessment identified areas of significant risk.

Coalfire's recommendations helped prioritize goals and secure funding for cyber risk management.

CLIENT CHALLENGE

Like many organizations its size, this investment firm relied heavily on third-party IT service providers, and assumed passwords and firewalls provided adequate security. After attending an industry conference, senior management recognized that existing security controls might not sufficiently meet the increased scrutiny by regulatory bodies, specifically the SEC and FINRA, as well as a growing list of clients and prospects. Management needed an objective, third-party assessment of risk and controls maturity to prioritize remediation projects and make wise investment decisions.

APPROACH

Engaged Coalfire as an independent assessor organization.

1. Conducted a gap analysis to compare the firm's current cybersecurity program against the standards in the NIST Cybersecurity Framework (CSF), v1.0.
2. Tailored an analytical approach to focus on items of high interest to regulators.
3. Developed a corrective action plan for significant control deficiencies.

**NIST CSF
security
functions**

Identify



Protect



Detect



Respond



Recover

EXECUTION

Over a three-month period, Coalfire's assessment consisted of technical testing, document review, observation, and inspection. The assessment considered all five security functions provided in the NIST CSF and mapped that framework to the SEC and FINRA's examination priorities. Coalfire interviewed personnel, gathered evidence, and walked through the environment to determine gaps in the firm's documented policies and provide associated remediation recommendations. From there, Coalfire reviewed current systems to determine whether the firm is following stated process and procedures.

RESULTS

The final report provided senior management with an accurate, reliable, and defensible assessment of the firm's current cybersecurity posture. Recommendations were specifically tailored to reflect the firm's reliance on third-party IT support contractors. Senior management was able to set meaningful goals and provide adequate funding to enhance the security program. The firm now has a clear path to a more mature cybersecurity management model and can better articulate security requirements to IT support contractors.

COALFIRE

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

Follow us to get the latest updates: [f](#) [t](#) [in](#)

Copyright © 2016 Coalfire Systems, Inc. All rights reserved.
Coalfire is a trademark of Coalfire Systems Inc.

CS_InvestFirm_07182016