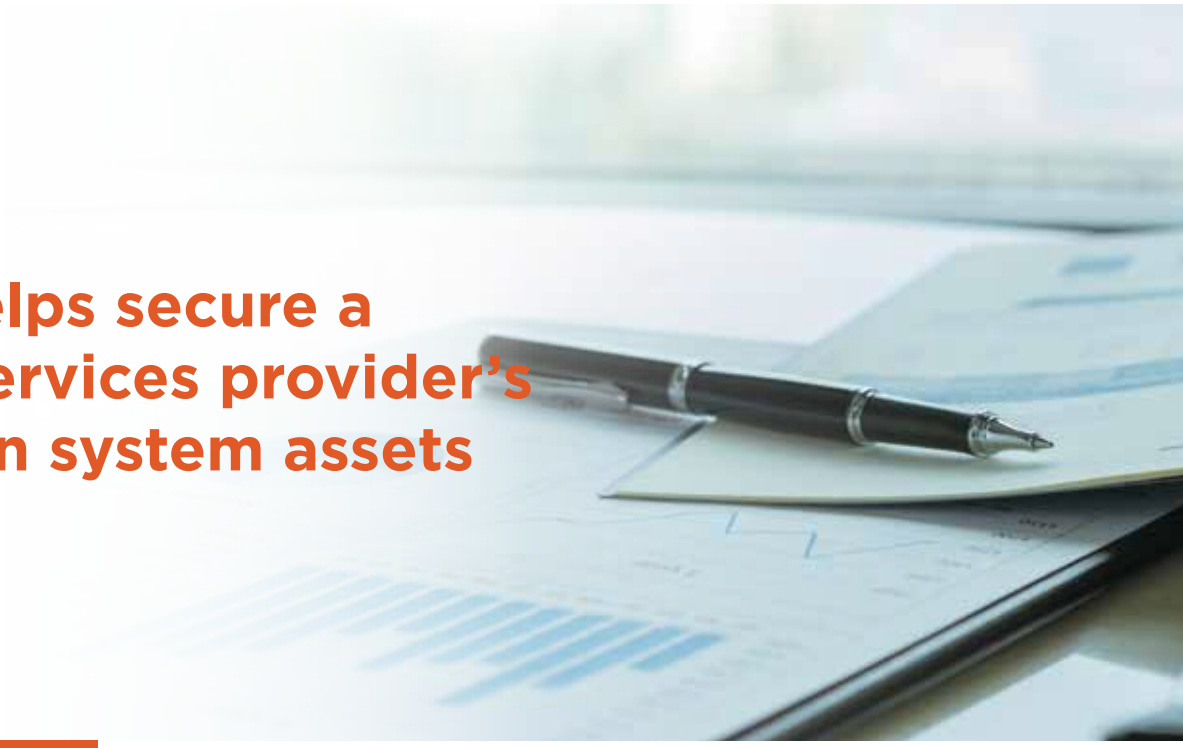
COALFIRE

CASE STUDY

Coalfire helps secure a financial services provider's information system assets



AT A GLANCE

A financial services provider in private equity, debt, and real estate financing recognized its vulnerability to a cybersecurity attack, and decided to benchmark against the industry best practice, NIST Cybersecurity Framework (CSF).

CHALLENGE

A financial services firm's senior management recognized that the organization was vulnerable to a variety of security threats. While the firm had a skilled and experienced cybersecurity team, management also recognized that additional security controls were essential to aligning with the best practice model, the NIST CSF, and continuing to improve its security program.

When the organization received notice from the U.S. Securities and Exchange Commission (SEC) that foreshadowed increased regulatory scrutiny, management needed an objective, third-party assessment of its security controls, and started a search for an independent global cybersecurity partner. After a few discussions, the organization was convinced Coalfire was best suited to solve its challenges due to the caliber of Coalfire's professionals, pricing, and ability to collaborate to find a solution. Coalfire was engaged to independently assess and benchmark the current security program to the controls inherent in the NIST CSF, identify and prioritize gaps, and develop a corrective action plan to address control deficiencies. The objective was to set the firm on the path to sustained cybersecurity program maturity, securing its most valuable information system assets.

APPROACH

Over a six-month period, Coalfire assessed security practices and related governance provisions, performed technical testing, and inspected system configurations. The assessment considered all five control stages in the NIST CSF (identify, protect, detect, respond, and recover) and each of the 96 subcategories, mapping that framework to the guidelines provided by the SEC. Coalfire collaborated with the firm's stakeholders to understand the current security and compliance landscape, by reviewing existing documentation and gathering evidence to support the identification of gaps and opportunities. Coalfire also assisted the client with building a security program to address the identified gaps.

RESULTS

Coalfire's efforts demonstrated not only the current risk posture, but also the financial and non-financial implications to the firm's business. Coalfire's report provided senior management with an accurate, reliable, and defensible assessment of the organization's current cybersecurity program. Multiple strategic and tactical recommendations helped set meaningful targets and secure adequate funding for improvements to the firm's security program.

Since the initial engagement, a Coalfire-led validation process has become an integral part of the firm's annual security and compliance process to track and sustain overall performance and measure its progress in reducing cybersecurity risk. The organization now has a clear path to cyber maturity and continued compliance with applicable SEC rules.

CS_CRA_FinSVP_080917

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com