COALFIRE®

Coalfire assists state government healthcare authority with building a powerful cybersecurity framework

AT A GLANCE

A state governance healthcare management and oversight agency for provider groups, payer groups, and other healthcare stakeholders in the midwestern United States handles significant volumes of protected health information (PHI) data and other sensitive data.

CHALLENGE

Given the agency's role in the healthcare industry, the company had to comply with HIPAA obligations, as well as the Minimum Acceptable Risk Standards for Exchanges (MARS-E).

Coalfire's compliance assessment team was engaged to conduct an initial assessment of controls relative to MARS-E. The results showed significant security gaps, prompting the state agency to begin taking a comprehensive approach to security management. Because of the MARS-E engagement, the organization partnered with Coalfire's cyber risk advisory team to combat the organization's cybersecurity challenges. The organization lacked an enterprise cybersecurity strategy and governance framework to effectively manage cybersecurity risks. Consequently, a formal enterprise security program was non-existent, and there weren't any clearly defined roles and responsibilities. Coalfire was engaged to help build out a formal enterprise cybersecurity strategy and governance framework.

APPROACH

Over three months, Coalfire's cyber risk advisory team engaged with the agency to define and document a formal enterprise cybersecurity strategy and governance framework. The project entailed developing a formal enterprise cybersecurity strategy and associated governance provisions to facilitate proactive risk reduction, quality security management delivery, and the appropriate use of resources in enterprise security management.
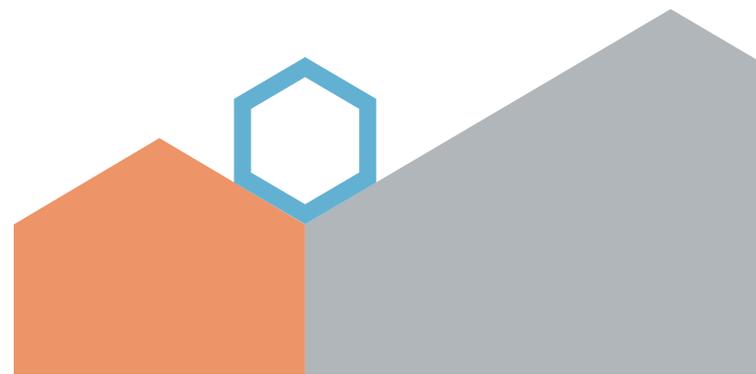
Coalfire's team reviewed the environment to ascertain strategic goals, complete a SWOT analysis, and define goals and objectives for effective security and compliance management. Multiple discussions and interview sessions were held with various stakeholders and executive leaders. From those discussions, Coalfire developed an enterprise security policy with associated standards, processes, procedures, management controls, risk, and performance indicators/metrics for the state agency. The resulting outcomes were socialized with key stakeholders and executive leaders for review and approval, and then a roadmap was prepared to guide the implementation of the strategy and associated provisions documented in the enterprise security policy, associated standards, processes, procedures, etc. Also, as part of the engagement, Coalfire defined a security operating model for the agency, incorporating strategic and tactical roles and responsibilities essential toward sustaining the quality of the agency's security program development efforts.

RESULTS

Coalfire concluded the engagement by conducting an executive presentation of the overall results, highlighting opportunities for efficiency in embedding security-related compliance obligations into the overall delivery of the security program. The presentation was well received by the agency's leadership team and culminated in the award of additional long-term advisory services to support the full operationalization of the enterprise security strategy and program and training of relevant personnel to assume their security-related roles and responsibilities.

Ultimately, Coalfire's efforts set the stage for the implementation of a full enterprise security strategy and program. The agency established an enterprise cybersecurity governance committee that will oversee and promote the pursuit of the agency's objectives for cybersecurity and IT compliance. Coalfire continues to be involved with the agency's MARS-E compliance and remediation effort and building and operationalizing the organization's security program.

CS_StateGovtHlthFramework_073117

COALFIRE.

About Coalfire