COALFIRE

CASE STUDY

Global manufacturing and retail provider relies on Coalfire to help improve cybersecurity maturity

AT A GLANCE

A global manufacturer and retail provider with more than 110 outlets worldwide and over $300 million in annual revenue was struggling to improve its enterprise security program in conjunction with its compliance program. Thus, they decided to conduct a cyber risk maturity assessment.

CHALLENGE

This global manufacturer and retail provider had put security practices and controls at large on the back burner, with most security operational tasks performed on a part-time basis by IT operations personnel. Subsequently, the organization failed to honor its Payment Card Industry (PCI) compliance obligations and was the subject of a significant security breach, without any formal security function or team in place to lead/support security management operations.

As a result, significant regulatory pressure was brought to bear, emphasizing the urgency of complying with relevant PCI regulations and establishing a sustainable framework to secure information and related assets. The PCI compliance challenges and lack of visibility into the environment also heightened executive leadership's concerns about paying hefty regulatory fines/penalties and its susceptibility to additional security breach attacks.

To help address those concerns, the organization started a search to find a globally trusted cybersecurity partner. Coalfire was subsequently recommended by a member of the client's Board

of Directors, who was familiar with Coalfire's service capabilities and quality of work. After a few discussions, the organization was convinced Coalfire was the right choice for a variety of reasons, including Coalfire's experience addressing similar challenges, the structured approach and methodology, the caliber of cybersecurity leaders and professionals chosen to assist the client, and pricing.

APPROACH

The organization engaged Coalfire's cyber risk advisory team to review and assess the current security operating environment through a cyber program maturity assessment. At the same time, Coalfire's qualified security assessor (QSA) team was engaged to define the scope of the cardholder data environment as a first step toward addressing PCI requirements. The outcomes from both exercises defined priorities for PCI compliance remediation efforts and set the stage for a more mature cybersecurity program and controls implementation.

Both Coalfire teams collaborated with the organization to discover existing cardholder security controls and benchmarked these against applicable PCI requirements to determine controls that were not satisfied. Both teams identified and scoped remediation efforts, and then defined, designated resources for, and executed a comprehensive PCI compliance remediation plan. Coalfire also assisted with a proactive communication mechanism directed at the company's regulators and cardholder processing partners to demonstrate commitment and progress toward achieving PCI compliance. The ensuing results and overall progress were continuously tracked and reported to the client's leadership team. Over six months, Coalfire's approach and advisory support ultimately led to the full remediation of PCI compliance gaps, resulting in the successful completion of a PCI-DSS facilitated self-assessment exercise.

RESULTS

As a result of Coalfire's efforts, the organization formalized and implemented various policies, standards, and processes. A significant number of tactical solutions were successfully implemented to "harden" the cardholder data environment and ensure the adequacy of security controls for the collection, use, and disposal of cardholder data.

Coalfire also:

- Designed, developed, and delivered training sessions to various stakeholders supporting retail, e-commerce, and technology operations that impact the client's cardholder data environment.
- Managed communications to the company's regulators and cardholder processing partners in ways that continuously demonstrated commitment to compliance.
- Established the framework, facilitating long-term sustainment of compliance.
- Implemented a governance model to enable continuous leadership visibility into the organization's security and compliance risks.

Ultimately, the organization was better positioned to pursue and achieve its strategic business objectives. Coalfire continues to provide advisory services to cover the organization's security and reduce related risks.

CS_CRA_GlobalManu_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