CASE STUDY

INTERNATIONAL RETAILER **SIGNIFICANTLY REDUCES RISK EXPOSURE** WITH COALFIRE

RESULTS AT A GLANCE

- 120 high priority cyber security risks were discovered
- 40% of findings were resolved in the first year
- Coalfire closed the gap in 50% less time and 75% less money than competing bids promised

CLIENT CHALLENGE

A US based retailer with over 700 locations internationally, engages Coalfire annually to audit and verify its compliance with PCI DSS requirements for its cardholder data environment (CDE). Coalfire reports demonstrate that the company has a strong PCI compliance program, but the company wisely wanted to evaluate its overall exposure to cyber risk. To do so, the Chief Legal Officer commissioned an assessment and penetration test of the corporate environment. That report highlighted an inconvenient reality: the company had significant risk exposure and rated well below its industry peers.

APPROACH

In order to reduce risk exposure and better align with industry peers, executive leadership engaged outside legal counsel for guidance. This guidance led to the solicitation of proposals to cyber advisory firms to lead a 2-year cyber risk reduction program. Upon careful review and consideration, Coalfire was selected to guide the program through resolution of the identified findings.

EXECUTION

During the initial phase, Coalfire created a security governance framework and organized a committee of key stakeholders to oversee the program. A Cybersecurity Program was developed, leveraging industry preferred security controls frameworks.

The various findings were then prioritized and categorized into domains, then aligned to specific projects under the Cybersecurity Program. The Cybersecurity Program and supporting projects were presented to the newly formed governance committee and received unaninmous approval. A Coalfire team was mobilized and deployed to begin working with internal resources, external vendors, and system integrators on risk reduction activities.

RESULTS

Approximately 40 percent of the findings were resolved in the first year. Among those corrective actions was the establishment of Incident Response and Forensic Investigations capabilities. These projects paid immediate dividends and enabled the company to rapidly respond to two cybersecurity events: ransomware attack and a fraud inquiry. In both instances, the company was able to investigate, respond and recover for from the alerts, and the company incurred no economic losses.

Year two of the program will bring closure to the remaining findings, which at the inception of the program totaled nearly 120 high priority items. The gap closure timeline designed by Coalfire was 50 percent shorter, and associated costs nearly 75 percent less than competing bids.

COALFIRE

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

Follow us to get the latest updates:

CS_InternationalRetailer_05182016