CASE STUDY

COALFIRE HANDLES A RANSOMWARE ATTACK WHILE **DEVELOPING AN INCIDENT RESPONSE PLAN** FOR AN INTERNATIONAL RETAILER

RESULTS AT A GLANCE

- Level 1 merchant was lacking in Incident Response capabilities.
- Coalfire was engaged to develop, implement and test an Incident Response plan.
- Ransomware attack on critical reporting systems during the project.
- Incident served as initial test of IRP in development.
- Successful adoption of plan by company's Cybersecurity Governance Committee.

CLIENT CHALLENGE

Coalfire annually engages a large global retailer with operations across the U.S. and in over 700 locations around the world. As a trusted partner, Coalfire verifies the Level 1 Merchant's compliance with PCI DSS requirements for its cardholder data environment (CDE). During our work, we identified that the Merchant was significantly lacking in its Incident Response capabilities. Executive leadership determined the need for a robust, scalable, and resilient Incident Response program, capable of contending with known and unknown threats and attacks.

APPROACH

Coalfire was engaged to develop, implement, and test an Incident Response plan. Coalfire began its work by leveraging processes already defined for the PCI environment and adapted best practices from NIST SP 800-61 as appropriate for the client environment. Coalfire also helped define the Incident Response Team, an incident classification scheme, and the procedures for use in various circumstances.

EXECUTION

During the development of the Incident Response Plan (IRP), there was a ransomware attack on a critical financial reporting system. Although the IRP was still in development, the company was able to leverage key process elements to isolate the infected systems, perform forensic analysis, eradicate the ransomware and return to normal business operations. Coalfire provided advisory services through the identification, response, and recovery phases of this incident, leveraging this situation as an initial test of the still in development IRP. These activities occurred with very limited interruption to the overall business.

RESULTS

Coalfire worked with the company to document the procedures facilitating the efficient response and recovery and identifying opportunities for improvement. Throughout the development process, key internal stakeholders were engaged to ensure appropriate IRP team skills and capabilities were deployed. Once the IRP was completed, the company's external legal counsel was engaged for review and approval, which then was presented and adopted by the company's Cybersecurity Governance Committee.

CS_IRP_08182016

COALFIRE

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

Follow us to get the latest updates: