CASE STUDY

HEALTH INSURANCE PROVIDER GOES BEYOND **COMPLIANCE WITH CYBERSECURITY**

RESULTS AT A GLANCE

- Health Insurance Provider needed to secure more than Protected Health Information.
- Coalfire conducted cyber risk assessment to determine risk posture.
- Evaluated cloud-based systems of Amazon Web Services.
- High-risk items uncovered requiring immediate attention and fixed in short order.
- Overall, nearly 100 medium-high and high vulnerabilities were discovered.
- Coalfire created a prioritization matrix to guide remediation efforts.

CLIENT CHALLENGE

A rapidly growing healthcare insurance provider successfully compliant with HIPAA/HITECH requirements, needed to secure more than just Protected Health Information stored on their systems. It was also imperative that they secure the remainder of their corporate environment, including all Personally Identifiable Information, client and trusted third party data.

APPROACH

The company selected Coalfire to complete a cyber risk assessment of key internal systems and information assets to determine their current risk posture and ensure compliance with industry standards. This assessment leveraged NIST-based frameworks (Cybersecurity Framework v1.0, SP800-30, and SP800-53 Rev 4) to determine current risk posture and prioritize vulnerabilities for remediation. Upon completion, Coalfire presented the findings and a prioritized remediation plan to executive leadership.

EXECUTION

The company utilizes Amazon Web Services (AWS) as their primary infrastructure for delivering services to their customers. This presented a unique challenge, as it was not possible to evaluate the physical data center controls. Coalfire's response was to evaluate the cloud based systems, applications, infrastructure, the associated configurations and system interactions. Additionally, physical controls of two office locations were assessed, with one of the locations housing call center support systems and personnel.

Coalfire identified mobile device management platform default setting that would allow the installation of unauthorized software by anyone. As a result, Coalfire immediately contacted the client, recommended a solution, and reviewed the fix within 24 hours. The remediation occurred during the assessment and had no impact to business operations.

RESULTS

Nearly 100 medium-high and high vulnerabilities were discovered. These were categorized and prioritized based on impact and level of effort to remediate. Coalfire then created a prioritization matrix, highlighting the top 10 risks, where remediation efforts would have the greatest positive impact on the company's risk posture. All findings and vulnerabilities were documented in a findings workbook, assessment report, and an executive briefing. The company was delighted with the output of the assessment and is working with Coalfire on additional cyber risk activities, including additional assessments and potential remediation work.

COALFIRE

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

Follow us to get the latest updates: