CASE STUDY

ECOMMERCE COMPANY SETS OUT ON A **PATH TO EFFECTIVE CYBER RISK MANAGEMENT**

RESULTS AT A GLANCE

- An initial needs assessment was required to create an effective cyber risk management.
- Coalfire identified critical information assets and the degree of vulnerability.
- Developed board presentation outlining analysis and recommendations.
- Coalfire staffed the project with a consultant who had previously served as CISO at an Ecommerce company.
- Board accepted the report without modification and extended analysis to other acquired operating units.

CLIENT CHALLENGE

The Board of Directors of this fast-growing, privately-held Ecommerce Company recognized that they are accountable for enterprise risk management, and they were particularly concerned about cyber risk, since one of their recent acquisitions had been victimized by a cyber incident. However, they hadn't yet appointed a Chief Information Security Officer (CISO), and they needed their technology leaders to stay focused on software development and production operations. The Board still needed information, so they instructed the head of IT Operations to find an experienced consultant that could complete an initial assessment and put the company on a path to an effective cyber risk management process.

APPROACH

After reviewing multiple proposals, the company hired Coalfire's Cyber Risk Advisory team. Coalfire staffed the project with a director-level consultant who had previously served as a CISO at an Ecommerce company, and a team of consultants with experience across multiple security and compliance domains. The team adopted a semi-quantitative approach to the risk analysis, based on NIST 800-30 guidelines, and developed a 6-week project plan. The team identified critical business processes, interviewed stakeholders, classified information assets, analyzed adversarial and non-adversarial threats, and gathered information on current security controls.

EXECUTION

Early in the project, it became clear that the company had many good security practices in place, but didn't have an over-arching security strategy, or even a clear understanding of what they were trying to protect. Thus, the Coalfire team took their analysis up a level, and helped the company identify eight particularly critical Information Assets and then consider the degree to which those assets were vulnerable to 20 of the most worrisome threats in the NIST taxonomy. Those ratings where then coupled with a business impact assessment to yield a current-state risk rating for each asset plotted on a 2-dimensional heat map (impact vs. likelihood).

Once this initial assessment was completed, Coalfire interviewed company leaders to gain an understanding of risk tolerance and risk reduction objectives. The team then drew on its knowledge of security best practices to define a targeted risk rating for each Information Asset and a Risk Register that defined tactics and projects needed to achieve the targeted state of cyber risk.

RESULTS

Once the analysis was completed, the project sponsor asked Coalfire to develop a presentation that he could share with the Board. The presentation included a business-oriented description of the cyber risk management principles and a portrayal of the team's analysis and recommendations. The Board accepted the report and immediately asked the sponsor to extend the analysis to two other recently-acquired operating units. In addition, the board decided to appoint a CISO and begin work on the projects identified in the Risk Register, and invited Coalfire to fill that role until a permanent CISO can be hired into the company.

COALFIRE

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

Follow us to get the latest updates:

CS_Ecommerce_05182016