CollegInvest couples compliance and security best practices to strengthen its posture

**AT A GLANCE**

CollegInvest, a not-for-profit division within the Colorado Department of Higher Education, gives individuals who want to save for college the ability to do so. The organization needed to comply with FISMA due to a government contract, but also wanted to ensure its enterprise was secure from the top-down.

**CHALLENGE**

According to the Verizon Data Breach Investigations Report, 93% of attacks against firms in the financial and insurance industry were financially motivated. To avoid becoming another statistic, CollegInvest decided to increase its security posture by conducting an annual security assessment with its need to achieve FISMA-ready status.

With little time wasted, CollegInvest selected Coalfire to provide a security assessment and a FISMA controls and documentation development review. “Our peers used Coalfire in the past and had great success” stated Jeff Gammon, CIO, CollegInvest. “We were very impressed with their technical expertise and ability to provide reports that were insightful.”

**APPROACH**

CollegInvest and Coalfire decided on a three-pronged security assessment approach consisting of internal and external penetration tests, vulnerability scans, and social engineering.

First, Coalfire performed external and internal network penetration tests against client-identified systems. Second, Coalfire performed a set of social engineering assessments to help evaluate the risk of an attack. Lastly, CollegInvest leveraged Coalfire’s powerful cloud-based vulnerability scanning tool, CoalfireOne™, to perform internal and external scans to identify potential vulnerabilities both inside and outside the organization’s network.
Shortly after the series of security assessments were complete, Coalfire started the second phase of the engagement with a FISMA documentation development review in which Coalfire assisted in the design and development of required policy documentation including the system security plan (SSP), business process recommendations, and a system contingency plan based on the agency’s requirement. CollegeInvest ended its engagement, with an FFIEC controls review, which helped the financial planner address the implementation of the controls found in the FFIEC information security examination handbook.

RESULTS

With Coalfire’s technical expertise and advice, CollegeInvest was able to substantially reduce risks for its business while progressing to the next phase of the FISMA process. “In addition to reducing risks for the business, we’ve been able to increase efficiency and resource productivity,” says Gammon. “With Coalfire’s help, especially with the security assessment, our resources have time back in their day to focus on business priorities. Ultimately, this engagement has allowed us to streamline our process and have more transparency into our security posture.”

“We continue to partner with Coalfire due to their impressive breadth of technical knowledge and actionable advice.”

JEFF GAMMON, CIO, COLLEGEINVEST

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 nearly 20 years and has offices throughout the United States and Europe. Coalfire.com

Copyright © 2018 Coalfire. All rights reserved.