Compliance Solutions Strategies

Regulatory Technology Driven by Data. Backed by Service.

Cybersecurity - Client Success

Market Landscape

The Securities and Exchange Commission (SEC) published a report on Cybersecurity and Resiliency Observations and several risk alerts in which it sets forth expectations for strong information security controls to combat the growing risks of phishing, ransomware, and credential stuffing, as well as increasingly sophisticated attack methods employed by cybercriminals. Our client is an adviser to private funds. The RIA was challenged to manage its own cybersecurity risk while simultaneously seeking to understand the cybersecurity risk profile of its portfolio holdings.

The Client:

Our client is an SEC-registered investment adviser with 85 employees across three U.S. offices. The RIA advises private equity funds in sectors which include manufacturing, healthcare, professional services, and real estate.

Business Challenge:

The Chief Compliance Officer (CCO), Chief Operations Officer (COO) and Chief Technology Officer (CTO) recognized the need to increase their cybersecurity defenses while trying to get a handle on the inherent cybersecurity risks in their portfolio company investments. The senior management at the RIA understood that breaches at the underlying portfolio company level could have a material impact on fund valuations in addition to operations and cash flow (in the event of network or system outages and ransomware). The firm had experienced several successful phishing attempts, including one in which funds were stolen. The firm's existing cyber policies were minimal, although some ad hoc control structures existed. The firm's appreciation of the risks to the business was enhanced by the current increased regulatory scrutiny around cybersecurity controls and an ever-expanding set of expectations from investors around privacy and security arising in the course of investor due diligence.

Business Results:

Using a combination of technology backed by in-house regulatory and cybersecurity expertise, CSS provided the RIA with a comprehensive cybersecurity risk management suite. The firm engaged CSS to conduct 24x7 dark web monitoring of its email accounts across several domains, using artificial intelligence and human interaction to present actionable risk intelligence in clear, understandable terms for senior management to reduce the risk that compromised credentials could be used against the firm. CSS rolled out a cybersecurity testing plan which included regular vulnerability scanning, penetration testing, phishing testing, and a combination of on-demand security awareness training modules and live, customized security training tailored to the firm's specific policies and procedures.

Value Realized:

The RIA was able to identify that 25% of its staff and 10% of its portfolio company employees were susceptible to phishing attacks and promptly remediate, saving the firm up to $5.86M in data breach costs. CSS testing identified opportunities to add Multifactor Authentication to applications, identified passwords which had not been changed in over a year, and its team developed a tailored set of information security policies and procedures that have helped the firm respond favorably to investor RFPs and DDQs to expand its investor base.

Don't wait until a cyber incident occurs.
Contact CSS's Cybersecurity Team today to see how you can achieve a cybersecurity program that showcases your strength and resiliency: **cybersecurity@cssregtech.com.**

Compliance Solutions Strategies