March 2019

WELLS FARGO SECURITIES

Wells Fargo Prime Services
Industry and Regulatory Updates

Previously published in Wells Fargo Prime Service's Industry and Regulatory Updates, March 2019 edition

Three Questions to Help Reduce Your Cyber Risk Today

By: Ezra Church, Partner, Morgan Lewis & Bockius LLP

2014 was supposed to be the "Year of the Breach"—that was the year the issue of cybersecurity really burst into our consciousness with major payment card breaches at prominent retailers. Five years later, and the statistics and costs involved in data breaches continues to be pretty staggering. According to statistics from the ID Theft Resource Center, in 2014, there were 783 breaches reported. Last year, there were 1,244 breaches reported.[1] Studies from IBM and Ponemon Institute show that the average cost of a data breach in the United States last year was $7.9 million with an average cost of $148 per record—$206 per record in the financial services industry.[2] With the increased risks and costs has come increased regulatory focus by the Securities and Exchange Commission (SEC) and other agencies, who—in the past five years—have made cybersecurity a centerpiece of guidance, examination, and enforcement efforts. The challenges involved can often seem overwhelming for businesses concerned about their exposure, particularly in the funds industry where the nature of the data and risks can be particularly acute. What the past five years have also shown, however, is that some of the most important things that you can do to help protect your organization and reduce cyber risk are the most straightforward. Here are three questions to ask and help take control of the risks at your firm.

Who's sweating cyber?

One of the most critical things you can do is ensure that there is an individual or team in place who has cybersecurity and incident response as part of their job responsibilities. In 2016, the SEC entered a settlement with an investment advisor, resolving charges that it had failed to protect confidential and sensitive customer data. The firm had a Written Information Security Policy ("WISP"), which is required for example under the SEC's Safeguards Rule, but failed to include some key information. One critical omission was the failure to identify who was in charge of security. The WISP stated that the "Designated Supervisor" was responsible for ensuring compliance with the policy, but didn't identify who the Designate Supervisor was. These failures were part of the SEC's decision to bring this enforcement action, resulting in a significant fine and obvious reputational harm to the organization.

Data shows that the concern on the part of the SEC is a real one. Year after year, the Ponemon Institute Study regarding costs of data breaches shows that the single, most impactful thing a company can do to reduce the incidents and costs of breaches is not extensive use of encryption, employee training, use of security analytics, participation in threat sharing—although all those things are helpful—but rather the simple designation of an incident response team. Organizations that take the time to designate an individual, or team of individuals, who are responsible for ensuring that the company is ready and responds appropriately in the event of a data breach will significantly reduce risk and impact associated with cybersecurity breaches.

Do we really need all that data?

Many funds collect personal and sensitive information reflexively without really thinking about it. Maybe it is the result of a form that has been used for years without revisiting—borrowed from consultant, former workplace, or found on the internet—adopted without really considering whether all the data is needed. One concrete, impactful step you can take now is to examine your data collection and retention practices and ask whether the data is something that is really needed. Perhaps it is better to forgo certain information and reduce the Firm's exposure to risks associated with that information. Do you really need to collect social security numbers? Could you collect just the last four digits? Could you collect them for required verification, but then delete them? Increasingly, the concepts of data minimization and firm limited retention periods are becoming legal requirements. For example, both concepts are critical to the EU's new General Data Protection Regulation. Again, asking these questions and making some decisions about how you collect and keep personal data is not particularly burdensome or cost prohibitive; but it is a step that can significantly reduce the risk profile of your firm.

What are our vendors doing with our data?

It now part of the privacy lawyer folklore that the 2014 Target data breach was supposedly started when a small heating and air-conditioning subcontractor in Sharpsburg, PA—a little town in western PA near Pittsburgh had their log-in credentials stolen. With those credential, the bad guys were able to access Target's system and push out malware to point of sale terminals throughout the country, allowing the collection of sensitive credit card information.

In the financial services space, the SEC has made clear that you cannot avoid responsibility for cybersecurity if the data is maintained by vendors. For example, in 2015, the SEC announced settlement with an investment advisor arising out of a breach involving data maintained on a third party-hosted web server. A cyberattack resulted in access to the personal data of more than 100,000 individuals. Vendor management has been repeatedly emphasized by OCIE as critical to maintaining appropriate safeguards.[3] Vendor management includes proper vetting at the outset of a relationship, contractual provisions

ensuring that the vendor will maintain the security of your firm's information, and routine monitoring of the vendor to ensure they are maintaining appropriate data security standards.

Cybersecurity is never done, the past five years of constant attention have shown that this is not a problem that can be solved, but one that requires regular attention. In a connected, technology-centric business world, the opportunities for cybersecurity attack, cyber-fraud, and other data breaches are a reality. But with these three questions, you can substantially improve your fund's compliance and reduce your risk.

BusinessConsulting@wellsfargo.com

www.wellsfargo.com/primeservices