CYBERSECURITY: A CRITICAL ELEMENT OF THE TRANSFER AGENCY OF THE FUTURE
The Threat

Between complying with Regulation S-P requirements, providing satisfactory answers amid board and investor scrutiny, and ensuring your firm’s name doesn’t appear in a headline with the word “breach,” you need to put cybersecurity at the core of your transfer agency operation.

Attend any board meeting in the investment management industry, and you will undoubtedly see cybersecurity as a key focus of the agenda. Conduct a quick internet search for “cybersecurity in investment management,” and you’ll see over 100 million results. Peruse open job postings in the industry, and you will see “cybersecurity” as an increasingly popular keyword. There is no question that cybersecurity is one of the most significant areas of the investment management operation today, and for good reason. As just one example, from working with many investment management firms and transfer agency departments, we’ve seen that it isn’t uncommon to have hundreds or even thousands of attacks on a perimeter firewall every day. Cyber threats are all too real in today’s marketplace.

The Rules

To help markets keep pace with these threats, regulators are upping the ante for investment managers and all market participants to ensure stronger controls around their data, technology, procedures and processes. To wit, the U.S. Securities and Exchange Commission (SEC)’s spotlight on cybersecurity says, “As markets grow more global and complex, so too are the threats through cyber intrusion, denial of service attacks, manipulation, misuse by insiders and other cyber misconduct.” Among a number of regulations aimed at protecting investor data and advancing cybersecurity, Regulation S-P mandates that investment companies, investment advisers and registered broker-dealers “adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.”

In addition, the National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce, offers a true best-practice framework that organizations in our industry and beyond should use as the model to which they should evolve their cybersecurity practice. The Framework includes five key areas: identify, protect, detect, respond, and recover. However, we see many firms and service providers grappling with how to keep pace with cybersecurity regulations and advancements.

THERE IS NO QUESTION THAT CYBERSECURITY IS ONE OF THE MOST SIGNIFICANT AREAS OF THE INVESTMENT MANAGEMENT OPERATION TODAY, AND FOR GOOD REASON
The Questions

Layered on top of regulatory challenges are the increasingly frequent and high-stakes questions that transfer agents face from both boards and investors. Under the umbrella category of, “Can you prove our data is safe?” we see a variety of cybersecurity-related questions being thrown at our clients. Some of these questions include:

- What is your budget for cybersecurity protocols? And, what has the budget increase been year-over-year?
- Have we had any data breaches, particularly where non-public personal information (NPPI) has been accessed in an unauthorized manner, duplicated, or removed from the premises?
- Are we encrypting data at rest?
- How many attacks have you experienced over a given time period?
- Do you use white-hat third parties to come in and attack your perimeter in order to better understand your cybersecurity risks?

From what we have seen from partnering with our transfer agency clients and attending board meetings with them, these types of questions are top-of-mind for key stakeholders across the investment management ecosystem. If answering these questions leaves you feeling tense, you may need to skip the next section of this article.

The Headlines

Perhaps the greatest stressor for anyone involved in data management or cybersecurity is the underlying fear of having your firm named in a headline with the word “breach.” We have all seen headlines related to data breaches, abuse or misconduct, which leaves operations, technology and compliance leaders questioning, “Are we doing enough?”

Cyber risks and threats are ever-evolving, and if you have any doubt that your current cybersecurity measures are not as strong or robust as they should be, it is time to seek out a better partner for the future of your transfer agency.
The Answer

To ensure your transfer agency has the strongest strategy and process in place for cybersecurity, you need a partner that has a proven track record of going beyond the compliance and security basics.

FIS® Transfer Agency Services employs a “defense in depth” strategy to protect our clients’ data and financial interactions, including encrypting data at rest. Our multi-layer connects with each client’s ecosystem, and includes our FIS SaaS/cloud infrastructure layer, FIS applications and application security layer, FIS multi-factor authentication and authorization layer, FIS network security layer, and FIS communications security layer.

We use multiple compensating controls that prevent, detect and respond to threats against our clients’ data. Our “defense in depth” strategy utilizes a comprehensive set of network-based controls, end-user computing, asset discovery, preventative controls, production computing, production controls, and host-based controls to mitigate threats at every point.

In addition, Transfer Agency Services is part of FIS, a global fintech leader with a culture of compliance at our core, across people, process and technology:

People:
Our employees are held to a high standard in terms of security awareness, and we have FIS representatives that are part of a wide variety of industry and government partnerships and initiatives to stay ahead of cyber threat advances.

Process:
Our “defense in depth” approach was built on a bank security model, and our control environment is heavily reviewed by third parties – and we are consistently proud of our results.

Technology:
Our technology is built to be secure, and we continually invest in our solutions and our talent with respect to security and compliance, including running our Cyber Fusion Center, which greatly enhances our ability to thwart malicious activity.
The better transfer agency of the future starts with a hard look at cybersecurity today. With the right partner to power your operation and guide your security and compliance programs through an increasingly challenging environment, you will be one step ahead of the regulators, the board questions, and the headlines.

Visit our transfer agency website to learn more about Transfer Agency Services and put our team to the cybersecurity test.