The Misnomer about Cyber

Andrew J. Fotopulos & E.J. Yerzak

When investment advisers use the cloud, they are making a conscious, informed decision to outsource tasks to vendors who may have particular expertise or infrastructure in place to handle such tasks. From hosted email archiving to compliance reporting, and from hosted backups to client communication portals, moving data to the cloud can help many firms address business needs while enabling them to focus more on their core business – providing investment advice. However, the Securities and Exchange Commission has made it clear that while financial professionals can outsource processes, they cannot delegate the ultimate responsibility for the performance of those functions. After all, it is the investment adviser who is in the trusted position of a fiduciary with respect to the adviser's clients.

It is a mistaken assumption that if the cloud provider has a failure such as a data breach, outage, or failing to perform the contracted level of service, the cloud provider bears all the blame as well as all costs the adviser may suffer as a result of the vendor's failure. During our initial conversations with firms within the investment community, we discover a misguided belief that their liability is eliminated when utilizing a cloud provider. This article addresses that misnomer and ways to protect your firm.

From contractual arrangements pertaining to data breach expenses to encryption of data by cloud providers, and from written assurances to insurance, here are 10 tips to protecting and transferring risk.

1. Inventory and Classify Your Data

Know what data your firm collects, processes, and maintains. Does it contain personally identifiable information (PII) about your clients? Have you classified your data based on its contents (e.g. public, sensitive, or confidential)? In which states do your clients reside? State regulations may differ with respect to their definitions of PII.

2. Inventory Your Systems

Understand what computing systems you have, and where your data is stored on such systems. Which information is stored in which places?

3. Perform a Gap Analysis

Are your information safeguards for various systems commensurate with the level of protection required for the type of data stored on these systems? What do your policies and procedures require with respect to encryption and access controls? Are you complying with your stated procedures?

4. Identify the Business Need

If considering a third party service provider, establish a sound business case for the use of the vendor. Moving data to a hosted environment, for example, may save the firm money in terms of office space for server equipment and the need for in-house IT expertise to update and maintain the hardware. You may be considering the vendor to mitigate business continuity and disaster recovery risk because the vendor may have more resilient backup processes or be better positioned than your firm as an adviser to detect and respond to network intrusion events.

5. Know Your Risk Management Options

Risk assessments and gap analyses are useful in identifying the vulnerabilities and risks of your firm, and which can be addressed by implementing additional controls or outsourcing functions to a third party provider. Generally, risks can be addressed through four means: (1) avoiding the risk, (2) accepting the risk, (3) mitigating the risk, or (4) transferring the risk. Avoiding risk is difficult and generally involves abstaining from a line of business or practice associated with the risk. Third party service providers can assist in mitigating risk. Firms can also choose to transfer some risk to another party, such as through one or more insurance policies. Finally, firms may be forced to accept certain risks at the point when the cost of additional controls exceeds the expected liability for a security incident.

6. Map Data Flows and Information Sharing

Know what information you will be sharing with the third party service provider. Does it contain personally identifiable information (PII) about your clients? Does it contain sensitive intellectual property belonging to your

firm? If a breach does occur, you will want to know the general nature of the information which was compromised in order to properly assess response strategies.

7. Do Your Due Diligence

Your clients entrust you with their information, and they expect you to safeguard it from misappropriation and misuse. It is therefore critical that you perform adequate due diligence on any third party service provider you are considering granting access to this information. Ask sufficient questions in order to obtain assurances that the service provider will safeguard the data, such as the following:

- Does the vendor encrypt your data in transit and at rest?
- What is the vendor's privacy policy?
- Does the vendor have an adequate business continuity plan?
- What information security controls does the vendor have in place? Review the vendor's SSAE-16 or other similar internal controls report, if available to you.

8. Review Service Level Agreements

It is imperative that you review Service Level Agreements (SLAs) carefully and ensure that you understand what the vendor is promising in terms of uptime, availability, responsiveness. The contract negotiation stage is the best time to document in writing whether and how promptly the vendor will notify you in the event of a breach or incident impacting its systems, and which parties are liable for breaches and related expenses when the data is stored on the vendor's systems.

9. Monitor Third Party Providers

Ongoing monitoring and due diligence is essential to obtain assurances that your vendors are adhering to their SLAs, and that any changes in the vendor's business, operations, hiring practices, or financial condition do not adversely impact your firm's ability to serve your clients. Periodically assess whether your vendors have experienced any data breaches or cybersecurity incidents.

10. Consider Transferring Risk

After your firm's risks have been addressed through cost-effective controls, what remains is called residual risk. If the residual risk is more than your firm is willing to accept as within its risk appetite, transferring some risk to another party through one or more insurance policies may be appropriate. You may have coverage for certain types of risks under Directors and Officers (D&O) policies, Errors and Omissions (E&O) policies, and general liability policies. However, some specific risks such as cybersecurity breaches at your firm or at your third party vendors may fall outside the scope of coverage provided by these policies, and you may wish to consider a Cyber Liability Policy to offer protection to your firm. Please see the following discussion of important things to consider in a Cyber Liability Policy.

Understanding the Scope of a Cyber Liability Policy

Yerzak: Are regulatory defense costs, fines, and penalties covered under a Cyber Liability Policy?

Fotopulos: The answer is case by case or policy by policy. However, the majority of policies provide coverage for defense costs and fines/penalties for violations of privacy regulations, including the Identity Theft Red Flags Rule.

Yerzak: Is there first party coverage (financial harm to you, the insured financial institution) or third party coverage (damages to others based on your actions or inaction)? What about coverage for external hackers, coverage for malicious insiders, or inadvertent breaches by employees?

Fotopulos: Again, this is a (insurance) policy by policy consideration when determining which insurance protections to purchase for your firm. The policies for Cyber Liability are not generic and are ever evolving. Another issue to consider when deciding among policies is what coverage may already be in place under other insurance policies such as a Fidelity Bond or D&O/E&O Liability policy as to whether you need these coverages under your Cyber Liability Policy. For instance, the primary intent of a Fidelity Bond or Commercial Crime Policy is to protect your firm against financial loss due to a dishonest act of an employee. The D&O (Directors & Officers Liability) policy is designed to protect your firm against loss for issues such as lack of due diligence or breach of

duty by your firm and its employees. In other words, what due diligence have you done to ensure that your clients' personally identifiable information is secure with the vendors or independent contractors utilized?

Yerzak: What minimum insuring agreements should be included?

Fotopulos: Again, this is a factor influenced by the existence of other insurance contracts you may have in place. Some of the basic insuring agreements under a Cyber Liability Policy include Network Security & Privacy, Breach Response Costs, Network Asset Protection, Reputational Expense, Regulatory Defense & Penalties, Multimedia Insurance, as well as Cyber Extortion and Cyber Terrorism. Buyer beware, all insurance policies have an "other insurance" provision within the policy that states that their policy may not apply or only apply as excess to any other collectible insurance policy. Coordinating coverage can prevent disputes among carriers.

Yerzak: Does the adviser need to encrypt everything in order to be approved for a policy?

Fotopulos: Whether the insurance policy itself goes into "encryption" requirements or not, every policy has what we refer to as the "Uniform Commercial Code" Exclusion. Common policy language states, there is no coverage for loss based upon, arising from, or in any way involving the actual or alleged government enforcement of any state or federal regulation including, but not limited to, regulations promulgated by the United States Federal Trade Commission, Federal Communications Commission, etc. Article 4A, under the Uniform Commercial Code requires encryption when it comes to Wire Transfers.

Yerzak: Generally, who should report a cybersecurity incident to the carrier, and what is the timing for such reporting?

Fotopulos: There is no standardized wording but the more narrow the definition of "who becomes aware of the situation" before the reporting requirement kicks-in, the better. Some policies state that you have to report within 60 days when an employee becomes aware of the event that may cause a loss. If the event is not immediately brought to the attention of the person familiar with the insurance policy requirements, policy provisions may be violated thus void coverage. Other insurance policies state that the Risk Manager, General Counsel, or a senior officer or director of the firm must first become aware of the event before the reporting provision clock starts ticking. This is also where your firm's Written Policies and Procedures' escalation requirements need to be coordinated with your insurance policy reporting provisions. Coverage for forensic investigation and data breach notification costs are essentials when purchasing a Cyber Liability Policy, but you need to be aware of whether or not the limits are within or in addition to the policy limit of liability. Specific to data breach notification, there may be restrictions in terms of the number of individuals, records or a sub-limit of liability that applies.

Yerzak: Are policies calculated based on number of clients, number of records, number of employees, type of data?

Fotopulos: The insurance industry has not come-up with a unified method of determining the cost for this policy. Employee count, records, transactions, and annual revenues are some of the various factors insurer's utilize to rate a risk. The key is coordinating your various insurance policies to ensure you have the right protection for your unique risk and that the firm's Written Policies and Procedures are coordinated with your insurance policies. Due diligence is a continuous process and needs to be performed at many and various levels not only to properly protect your firm but you as CCO.

About the Authors

Andrew J. Fotopulos is President of Starkweather & Shepley Insurance Corp. of MA as well as their investment industry practice group managing director. Andrew has specialized in the insurance needs of the investment industry for almost 30 years. Celebrating 135 years in business, Starkweather & Shepley is the 69th largest insurance broker in the country providing all lines of commercial, personal lines and employee benefits insurance.

E.J. Yerzak is Vice President of Technology at Ascendant Compliance Management, Inc., a regulatory compliance consulting firm which performs risk assessments, annual reviews, due diligence reviews, and Information Technology Risk Assessments for investment advisers, broker-dealers, and advisers to private funds.