The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 21, NO. 12 • DECEMBER 2014

The Liability Hole — Cybersecurity Risks and the Apportionment of Liability

By Gwendolyn A. Williamson and Mary C. Moynihan

Suffice it to say, cybersecurity has been a hot topic in the mutual fund industry during the past year. Fund advisers and boards of trustees have awoken to the information technology (IT), data security and privacy risks faced by their funds; countless industry conferences and seminars have offered education on cybersecurity issues, including the haunting specter of state-sponsored attacks;[1] and the Office of Compliance Inspections and Examinations (OCIE) at the Securities and Exchange Commission (the SEC) has embarked on a mission to assess cybersecurity preparedness and threats in the securities industry by announcing examinations of more than 50 investment advisers and broker/dealers.[2] While this earnest focus on the IT-related risks of the modern securities marketplace is certain to benefit mutual funds and their shareholders, the question of who should foot the bill for fund losses caused by cybersecurity failures remains unanswered. This article first discusses the current liability landscape and steps that fund boards should take to understand their funds' potential liability in the current cyberthreat environment. It then suggests the types of contractual undertakings fund boards might negotiate with their service providers to clearly apportion risk. Finally, the article outlines the current options for and issues with obtaining insurance to cover gaps. Each of these steps is important to ensure that funds and their shareholders are protected from cybersecurity losses to the greatest extent possible.

Liability and Threat Landscape

1. Liability for IT Related Losses

The issue of liability for financial losses caused by cyberattacks is of particular importance to mutual funds and their primary service providers[3] whose IT systems may afford direct access to fund assets and are thus particularly susceptible to being targeted by internal and external bad actors.[4] The IT systems of asset managers and their service providers also house a myriad of sensitive data – including, among other things, fund portfolio holdings and trade data, proprietary research and in some cases personal identifiable information (PII) – all of which, if compromised, could expose funds and their advisers to losses from business interruption as well as civil litigation,[5] liability for violations of the federal securities laws,[6] violation of state privacy laws[7] and almost incalculable reputational harm. In addition, cyberattacks carry their own costs, in the form of expenses incurred to investigate, identify and repair damages to a firm's IT systems and data files.[8]

Funds and their shareholders may be protected from cyberlosses to a certain extent under their existing contracts with primary service providers. These contracts may indirectly address liability for fund

losses arising from IT system failures by imposing a general negligence or gross negligence standard of care on the service provider in the performance of its duties. But it is unlikely that any of a fund group's investment advisory, administration, distribution, transfer agency, custodian or, as applicable, securities lending, agreements directly address IT systems or contemplate liability for the potentially significant losses that a cyberattack could cause. Indeed, standard agreements are unlikely to even mention the operation and maintenance of the service providers' IT systems or the protection of digital data. Nonetheless, because the operation of IT systems and digital data underlie the performance of nearly all of the functions enumerated in fund service provider contracts, it seems likely that liability for cyberlosses is covered by the standard of care provided in the agreements. This seems a straightforward resolution of the more garden variety issues, such as systems going down or technology glitches, that the industry has dealt with for as long as it has relied on computers.

But what happens when, despite the reasonable best efforts of a service provider to impose industry standard or even "best-in-class" cybersecurity defenses, sophisticated intruders successfully access and misappropriate fund assets or confidential information? This is a real concern that fund boards and advisers must consider because, as recent attacks make clear,[9] even with a state of the art IT/data security program, a fund service provider might not even be aware that its cybersecurity perimeters have been penetrated. Indeed, losses arising from a successful cybersecurity attack are not likely to be the result of negligence on the part of the funds' adviser or other service provider, and since under most service provider agreements, liability is shifted to service providers only for fund losses arising from the service provider's negligence or gross negligence, the question of "who pays?" for fund losses arising from attacks on service provider networks (and those of their vendors) looms large.

Traditionally, the operations of a mutual fund complex have entailed relatively low risk. The net asset value (NAV) of shares is set daily and is based on the value of the assets held by the fund, which are typically liquid. The assets themselves are required to be held by a custodian bank, subject to a variety of specific regulations intended to safeguard the assets. Transactions in shares are performed through transfer agents registered with the SEC. Other than board members and perhaps a chief compliance officer, the fund itself has no employees. The greatest risk has been thought to arise from the occasional defalcation of funds and there are very few cases (with the obvious exception of the market timing cases)[10] in which funds have experienced significant losses. Existing service provider contracts and their liability standards work well in this low risk environment. Advisers and other service providers assume relatively little risk, because the risks themselves are perceived as low.

At the same time, while investors have understood that they assumed market risk (and all of the related investment risks that are detailed in fund prospectuses), the general assumption has been that investors assume very little operational risk. This is a function of the fiduciary and contractual duties of care, industry usage, and the heretofore low risk of any significant operational loss. Thus, for example, while an investor accepts the risk that the NAV of a fund may decrease, the investor typically does not accept, or expect to pay for, such things as trading errors, NAV errors (other than in a *de minimis* amount) or employee theft.[11] This is an important consideration in approaching cybersecurity risks. Failures of IT systems and resulting damages are operational, not market risks. Were a fund to experience a substantial loss related to IT failures, the industry's traditional approach suggests that the cost would not be passed on to shareholders; indeed, it seems highly unlikely that the SEC Staff would countenance such an approach.

This creates an interesting conundrum, or "liability hole." In the end, liability can be absorbed by

either the fund's assets or the balance sheet of the service provider (less insurance, as described below). Since a major cyberloss is most likely to arise in a situation in which the service provider has not been negligent, the service provider would arguably not be liable. At the same time, it seems difficult to argue that fund assets would or should be applied to cover losses that are fundamentally operational in nature.[12] A second issue to consider is that some statutes impose strict liability—for example, under certain state statutes, any loss of PII, regardless of negligence, results in liability to the firm holding the PII and may result in the assessment of fines as high as $1,000 per record compromised.[13] If the service provider is only liable for its negligence, and the contract provides an indemnification, the strict contractual analysis might result in fund assets being applied to pay applicable fines.

As discussed below, given this uncertainty, fund boards may wish to engage in discussions with their service providers to consider adjustment of contractual duties of care with respect to cyberlosses and seek to obtain appropriate insurance to cover any gaps. Many advisers have already assumed that they might bear the responsibility for cyberlosses, and they too would be well served by clarifying contractual liabilities and obtaining sufficient insurance. Without clear contractual assignment of risk and appropriate insurance coverage, an adviser's own balance sheet may be the only available source of funding for losses resulting from a significant data breach or IT network failure. Experience in other industries and with particular issuers who have faced complex questions of liability while in the midst of handling a major cybersecurity breach confirms that an ounce of prevention is worth a pound of cure.

2. Threats to IT Networks

As recently publicized breaches illustrate, the IT-threat landscape is extraordinarily dynamic, and fund service provider networks are vulnerable to both intentional attacks and security bugs/viruses introduced into their networks inadvertently. One veteran mutual fund chief information security officer has explained that the cyberthreat landscape varies from week to week depending on "what the other side of the fence is trying to do. Everything that's old is new again, everything from phishing and drive-by downloads and malware and advanced persistent threats to the standard rap-rap-rap knocking on the door of vulnerabilities like Bash, which has been out there for 26 years, and before that Heartbleed. There are a lot of different avenues we have to be on top of, as well as setting our road map in response to where we think it's going to go."[14] Indeed, the National Institute of Standards and Technology (the NIST) has acknowledged that risk management in the cybersphere entails "the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact."[15] The SEC has also suggested that fund boards should approach the IT-related risks of theft of fund assets, privacy/data security breaches, service breakdowns, and resulting regulatory violations as an ever-evolving, ongoing governance matter that must be managed and mitigated, and that mere compliance policies and procedures, while important, may be insufficient.[16] Putting in place contractual provisions and insurance coverage is an important way that fund boards can follow the SEC's guidance and move beyond risk assessment to actual risk management.

At the outset, it is important for fund boards and service providers to understand the risks they face, what their contracts say and the limits of their existing insurance coverages. Once these have been thoroughly mapped out, the parties can determine how to apportion risk and obtain insurance coverage, to the extent available. Towards this end, fund boards should first work to "map their data" by seeking to understand how the IT network that supports their funds' operations works and where critical data is located (both within the network environment and outside the network, to the extent housed through third-party vendors/sub-vendors). To conduct this

due diligence, fund boards should ask, along with any other questions they deem relevant:

Data Systems

- What fund information[17] flows through the network, and where is it collected and stored on the network?
- Who has control and operation of the network that supports fund operations? (Note that many IT systems are complex-wide and may not be under the unique control of a particular service provider within the complex.)
- What are the ultimate end points of the funds' digital data flow (that is, with whom is fund information shared, including with vendors), and how and why is fund information used at the various end points of the data flow?
- How many third parties have access to fund assets and/or data?
- Who is responsible for evaluating and overseeing, at the network level, the network environment and vetting or selecting the vendors/sub-vendors (including custodians and sub-transfer agents) and others who may gain access to fund assets and/or information?
- What is the process for ensuring that vendor/sub-vendor due diligence risk assessments and ongoing monitoring take into account specific business units' particular circumstances and usage of vendors and sub-vendors?
- What level of risk has been assigned to the vendors/sub-vendors that are most vital to fund operations? What criteria is applied to assign risk levels?
- Are there vendors/sub-vendors with access to the network that represent exceptions to the general security standards and policies applicable to the network, and if so, what procedures are in place to address the risks posed by those vendors/sub-vendors?
- How are patches, updates and antivirus protections managed?
- How is access to the network controlled?
- How are cybersecurity risks identified, and by whom?
- Who is responsible for responding to cybersecurity incidents/crises, and what procedures are in place for such responses?
- How frequently are independent cybersecurity audits and penetration tests conducted and what are the recent results? Do the service providers and vendors/sub-vendors regularly provide SSAE16 reports and related SOC1, SOC2, or SOC3 reports?[18]
- How do employee hiring, training and termination policies safeguard fund assets and data?
- How are physical facilities secured?

Contractual Provisions

- What protection from cybersecurity liability, if any, is available under existing service provider contracts?

Insurance Coverage and Other Sources Available to Cover Cybersecurity Losses

- What cybersecurity coverage is there, if any, under fund fidelity bond and E&O/D&O insurance policies and/or under service provider insurance policies, and how do these policies interact together, if at all, with respect to fund IT/data security matters?
- What is the financial condition of the adviser and its parent company, and to what extent could the balance sheet of these entities cover cataclysmic fund losses arising from a cybersecurity breach, including the theft of fund assets?
- What is the cybersecurity risk tolerance and posture of the board and of the funds' adviser and other primary service providers?

The answers to these questions will likely be complex, and it may take substantial time and effort for a board to ferret out all of the risks particular to its funds and the IT system(s) administered by their primary service providers. However, this due diligence is an essential inquiry to allow a fund board to

effectively work with counsel to negotiate the terms of cybersecurity liability agreements and insurance policies and to be sure that contractual provisions and coverage obtained complement actual service provider IT/data security programs. It may also provide important evidence that the fund board has engaged in appropriate oversight. Further, the answers to these questions may be central to the process of obtaining cybersecurity insurance coverage.[19] Insurance companies typically "scrutinize an organization's network security, privacy policies, password protection, intrusion detection, vulnerability scanning and incident response procedures."[20] Thus the underwriting process itself will likely help fund boards and advisers identify hidden holes in their cybersecurity protection and render the "firm better prepared to deal with a cybersecurity incident."[21]

Consideration of Contractual Provisions to Apportion Liability for Cyberlosses

The typical mutual fund family has different contracts with each of its primary service providers, some or all of whom may be affiliated, which typically apply a negligence or gross negligence standard to performance of the duties described in the contract.

As noted above, the negligence or gross negligence standard seems sufficient to deal with "business as usual" IT matters. However, fund boards and service providers should consider whether to enter into separate agreements or understandings covering liability for significant cybersecurity failures or data breaches where the negligence or gross negligence standards may be inadequate. Depending on the affiliation of a fund group's primary service providers and other factors, it may be most efficient for a fund board to seek to incorporate IT/data security protections into each of the funds' existing primary service provider contracts, or it may be more appropriate for the board to seek to enter into a stand-alone agreement or side letter with each service provider, or in the case of affiliated entities, their parent company, that delineates responsibility and liability for cybersecurity issues.

Each fund group's cybersecurity contract should, of course, be tailored to its operations and other unique circumstances. However, fund boards generally may wish to consider contractual provisions that:

- identify and assign ownership of all digital data and information stored on the service provider networks(s);
- establish that service providers have a duty to protect all digital data and information belonging to the funds;
- describe the circumstances under which service providers may collect, store, access, use, process, maintain and disclose fund information and ensure that this is consistent with policies on portfolio holding disclosure, codes of ethics and fund privacy policies;
- require service providers to develop, implement and continuously monitor and update industry-standard[22] physical and technical safeguards, an industry-standard written IT/data security program,[23] and an industry-standard network security program;[24]
- make clear that each fund service provider is fully responsible for the acts and omissions of its employees and agents as well as the acts and omissions of any vendors/sub-vendors or other third party it may engage, regardless of whether or not the fund service provider was aware of, or negligent or otherwise culpable with respect to, the matter in question;
- detail the level and methodology of due diligence that each service provider must conduct with respect to vendors/sub-vendors and other third parties that may be given access to information/data belonging to the funds, and, as appropriate, require that contracts entered into by service providers with third parties include controls and other safeguards against the unauthorized access to and use of fund

digital data and information that are at least as stringent as those applicable to the service provider;

- require each service provider to immediately provide notice to the funds of any unauthorized access to fund digital data and information and of any actual, probable or reasonably suspected breach of the network, and to promptly investigate and remediate any actual breach of the network;
- call for each service provider to arrange for and submit to the funds on an annual, or more frequent if appropriate, basis audit reports prepared by a qualified, independent third party regarding the service provider's overall IT/data security program, including a SSAE16 or higher;
- mandate that each service provider will (i) through a qualified, independent third party conduct cyber and physical perimeter testing at least annually, and more frequently as circumstances may require, and (ii) timely provide the results of such testing to the funds in a report that, at a minimum: identifies any material security gaps, vulnerabilities or other weaknesses; describes the nature of such IT/data security exposure; and certifies in writing how the service provider has corrected the shortcoming(s);
- provide that, in the event a cyberattack or other IT security incident requires the funds to provide notice of the breach to any foreign or domestic governmental entity or other authority, each service provider, at its own expense, will prepare and deliver such notice on behalf of the funds; and
- indemnify the funds and their officers, directors, employees and agents against *all* liabilities (including, but not necessarily limited to, disbursements, claims, losses, damages, penalties, actions, suits, judgments and liabilities[25]) arising directly or indirectly from any unauthorized access to or acquisition, use, loss, destruction, compromise, modification, or disclosure of any of the funds' digital data or information, including, but not limited to, PII, or interruption or disruption of the ability of a service provider to perform contracted for services, including the processing of redemptions and valuation of fund shares.

Fund boards should also keep in mind that because cybersecurity threats are almost constantly evolving, even with the most advanced IT/data security program currently available, service providers cannot foresee or prevent all of the cybersecurity risks faced by funds. As the authors of the Department of Homeland Security (DHS) Cybersecurity Framework concede, even their "comprehensive set of standards may not protect against sophisticated threats, such as those from nation-states and organized crime. This is the difference between compliance and security, and closing this gap requires action by boards and executives."[26]

The Case for Cybersecurity Insurance

The current insurance coverage status quo for the majority of mutual funds includes fidelity bond and D&O/E&O insurance policies. A fund group's fidelity bond, which is required by Rule 17g-1 under the 1940 Act, could potentially cover losses related to theft or other bad acts of a fund employee or officer perpetrated through a service provider's network, but typically would not extend to criminal or other acts of third parties. Moreover, under Rule 17g-1, the required coverage amounts would be woefully inadequate to cover any significant cyberloss. A fund group's D&O/E&O insurance is designed primarily to protect the funds' directors and officers, and provides only very limited coverage to the funds themselves. It is also relatively rare for a fund group to have a separate cybersecurity insurance policy, and fund service providers' existing insurance policies may not specifically address IT-related losses. Even when advisers and other fund service providers, and/or their parent companies, carry insurance that contemplates IT-related losses, it is not always the case

that the funds are named as "additional insureds" or covered as clients of the service provider. This situation poses the glaring question of what will happen in the event of catastrophic harm to a fund group due to an IT/data security breach? As noted above, cybersecurity attacks are not likely to be the result of negligence on the part of the funds' adviser or other service provider, and efforts to shift liability through contract may meet with varying success. Insurance may be needed to fill the gap.

The current dearth of mutual fund cybersecurity insurance coverage, coupled with the fact that the SEC is unlikely to allow funds and their shareholders to absorb losses arising from the operation of a service provider's IT infrastructure (which may include third-party vendor and sub-vendor IT systems), suggests that the balance sheet of a fund group's adviser and/or its parent company is the ultimate backstop against a cataclysmic cyberattack. This may not unnerve fund boards whose adviser and other service providers have deep pockets. But for many fund groups, the overall financial health of the adviser organization is not necessarily strong enough to weather substantial fund IT-related losses. There are currently billions of dollars in U.S. mutual fund assets that are susceptible to cyberattacks, but not insured against them. By seeking to obtain cybersecurity insurance coverage for a fund group and/or by insisting that the funds be included as named insureds, if possible, under service provider cybersecurity coverage, fund boards may be able to significantly reduce the risk of disastrous losses to shareholders.

Obtaining cybersecurity insurance can also yield funds and their service providers certain collateral benefits. The SEC has asked firms to disclose any relevant IT/data security related insurance since 2011.[27] Highlighting the existence of such coverage in fund registration statements, shareholder reports, and other materials would both satisfy the SEC and potentially ease security/privacy concerns of existing shareholders and potential investors. Indeed, industry commentators have observed that maintaining "a robust cyberrisk management program will not only help ensure efficient operations, but will also play a role in crossing cybersecurity thresholds established by customers that would otherwise serve as a barrier to entry."[28]

Types of Cybersecurity Insurance. Generally speaking, first-party and third-party liability cybersecurity coverage are available in the current marketplace. First-party cybersecurity insurance covers losses incurred by the insured, for example a fund group's costs associated with: lost income and opportunities resulting from an acute or sustained network breach; destruction of critical infrastructure (hardware, software and other IT property); restoration of regular business and security operations following a DDoS attack or other network security breach or interruption; legal, forensic, shareholder notification, crisis management and reputation repair services; cyber-extortion; and, potentially, theft of assets. First-party cyberinsurance can also cover contingent business interruption expenses when a cyberattack is directed against a third party involved in the insured's service chain.[29] Third-party cybersecurity insurance covers losses to third-parties for which the insured is liable, for example a fund group's costs associated with (i) regulatory investigations, actions and fines and (ii) civil class actions and other litigation brought by third parties against the funds alleging a violation of securities laws (particularly those relating to disclosure), breach of privacy, violation of privacy laws, or breaches of obligations to protect investors' confidential information, including any resulting judgments, awards or settlements.

It might be appropriate for a fund group to obtain both first and third party insurance closely aligned with its specific network environment and risks. Or, if the fund group's cybersecurity risks are particularly low, or risk tolerance is particularly high, a fund board might opt to obtain cybersecurity insurance that covers only PII or only the most sensitive and/or crucial fund trading data exposed through service providers' IT networks. Fund boards may also wish to assess whether their

existing D&O/E&O coverage would apply in cases involving inadequacy of disclosure or regulatory investigation. Spreading coverage for potential fund IT-related losses across multiple policies held by fund service providers, under which the funds are named insureds, could also be an attractive option to fund boards and service providers. In fact, reports suggest that this might be the most feasible approach for large fund complexes. Currently, the most coverage a company can hope to acquire, using multiple underwriters, is about $500 million, which is significantly less than the billions of dollars' worth of coverage available in other areas, for example, property insurance. Whatever form a fund group's cybersecurity coverage takes, boards would be wise to make sure that it relates not only to primary service providers, but also to any vendors/sub-vendors and other third-party networks with access to fund assets and/or data.

Potential Barriers to Cybersecurity Insurance. Fund boards should also be aware of certain potential obstacles to obtaining cybersecurity insurance. Most importantly, current offerings are limited. It is also generally difficult to determine the proper coverage amount for a company's cybersecurity policy because, outside of the funds' level of assets under management, limited information exists regarding the potential scale of loss. One way to estimate the proper coverage amount is to look at the losses and expenses borne by peers and other companies who have had breaches, but at this point in time, such data for the mutual fund industry is lacking. Additionally, it can be extremely challenging to accurately value the damages a fund group might experience as the result of a cybersecurity incident, which include reputational harm, lost opportunities, and liability for public dissemination of private information; as a result cybersecurity premiums are likely to be high.[30] As an industry observer points out, "the main problem is quantifying losses from attacks, because they are often intangible — lost sales or damage to a brand name, like the public relations disaster Target suffered after the breach of its point-of-sale systems late last year. At the same time, underwriters lack the data they need to figure out how likely it is that an attack will occur, or what it will cost. This is because most breaches go unnoticed or are never publicly reported. Information on past attacks is not particularly helpful because attackers are always getting more advanced, and the risk is increasing as companies put their most valuable data online."[31]

Beginning in October 2012, the DHS's National Protection and Programs Directorate (the NPPD) held a series of insurance industry workshops "to examine the current state of the cybersecurity insurance market and how to best advance its capacity to incentivize better cyberrisk management."[32] These workshops focused on the challenges involved in the current first-party cybersecurity market, and identified "lack of actuarial data and consequence-oriented analytics" as significant "obstacles to market growth," along with "the overarching need for infrastructure owners to build effective cyberrisk cultures as a prerequisite to expanding coverage."[33]

In the report that resulted from these workshops, the NPPD explained that "the first-party cybersecurity insurance market is a nascent one, particularly when it comes to coverage for cyber-related critical infrastructure loss. Carriers cited several reasons for their limited offerings in this area, chief among them being: a lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyberthreat vectors. Based on input from event participants and on its own research, however, NPPD identified three areas where it appeared progress could lead to more robust first-party coverage – not only for economic and intangible harms such as lost profits arising from "out of service" critical infrastructure, but also tangible harms involving damage to and/or the destruction of that infrastructure."[34] These areas include: (i) "the creation of an anonymized cyberincident data repository," which could "spur the development of broadly accessible cyberrisk actuarial data needed to advance the cybersecurity insurance market more comprehensively" and also allow firms to "benchmark their organizations'

current cyberrisk management performance against their peers;" (ii) "enhanced cyberincident consequence analytics," which could help underwriters "better understand the value of critical infrastructure and who might pay a premium to restore it" and also assist firms in developing "parallel tools that help determine both the likelihood and the probable consequences of a cyberincident to [their] particular organization;" and (iii) "enterprise risk management evangelization" that folds cybersecurity risks into a firm's overall ongoing risk management strategy.[35]

Future Outlook for the Cybersecurity Industry. Despite its growing pains, the market for cybersecurity insurance appears to be a quickly growing segment of the insurance industry. "Specialized policies to protect against online attacks are offered by about 50 carriers, including big names like the American International Group, Chubb, and Ace. As data breaches have become a reality of the business world, more companies are buying policies; demand increased 21 percent [from 2011 to 2012]."[36] Another major provider is Beazley. The Ponemon Institute reports that roughly 30 percent of US companies currently have some sort of cybersecurity insurance policy, and an additional 10 percent plan to purchase cybersecurity coverage in the near future.[37] And, as Bloomberg News reports, the head of cybercoverage at Aegis London, which sells policies through Lloyd's of London, sees "cyberinsurance as a once-in-a-generation opportunity that is set for growth."[38] Based on statements made at the March 2014 annual Investment Company Institute (ICI) Mutual Funds and Investment Management Conference and elsewhere, it is also expected that ICI Mutual Insurance Company, which offers insurance tailored to the needs of the mutual fund industry, is exploring options for cybersecurity insurance.

Those who closely monitor the insurance and securities industries have found that "as boards of directors have become increasingly concerned about exposure to cybersecurity risks, cyberinsurance is becoming more prevalent, especially among financial firms. Just like flood, fire, and auto insurance, the idea behind cyber-insurance is to mitigate the risk and cost of a cybersecurity incident."[39] Experienced information security officers suggest that the difficulties associated with estimating cybersecurity costs may not be as pronounced in the mutual fund industry as in other industries.[40] And, as representatives of the mutual fund insurance industry indicated at the March 2014 ICI Conference, it is expected that available actuarial data will increase, and premiums will decrease, as more and more asset management firms seek out cybersecurity insurance policies.

Fund boards should stay abreast of developments in the cybersecurity insurance marketplace in the long term, and seek to obtain the best possible coverage for their funds in the short term. Depending on the terms and coverage currently available to a fund group and its primary service providers, fund boards should revisit fund cybersecurity insurance on at least an annual basis.

Conclusion

Internet-based technology has introduced incredible efficiencies, but also significant security risks, to the mutual fund and broader financial services industry. The appropriate allocation of liability for mutual fund losses attributable to cybersecurity risks is a complicated subject for which industry best practices have not yet been fully established. However, fund boards can and should be proactive in working to establish the parameters of fund liability for cyberattacks and other IT-related losses. Assessment of what these bounds should be entails risk-focused due diligence that takes into account the service provider (and third-party vendor/subvendor) network(s) through which fund assets and data may become vulnerable, as well as all protective network controls in place.

The allocation of cybersecurity risk away from mutual funds and toward their service providers is appropriate for a number of reasons. It is unlikely that the SEC and other regulators would tolerate funds and their shareholders bearing the brunt of losses related to failure of a service provider's IT

security program, even if such failure was not the result of negligence on the part of the service provider. Fund service providers are responsible for building and administering their networks and related security programs and for vetting and granting network access to vendors/sub-vendors and other third parties. While fund boards certainly play a key role in overseeing risks posed to fund groups by service providers' networks, funds do not control these systems and, in many cases, cannot even gain a fully transparent view of them. Funds thus cannot reasonably be expected to assume liability for losses associated with the operation of service provider networks.

Boards can seek to transfer the cybersecurity risk exposure inherent in modern mutual fund operations by contracting with primary service providers and obtaining cybersecurity insurance coverage. This is a likely difficult, but potentially vital, step for boards to take given the serious harm that cybersecurity breaches can cause. In considering these issues, fund boards should heed the summary of cybersecurity risks presented by the DHS: "similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers."[41] Given the imperative nature of managing this risk, fund boards should act promptly to begin discussions on liability with their funds' service providers.

Ms. Williamson is Counsel, and **Ms. Moynihan** is a partner, in the Washington, DC office of Perkins Coie LLP. They would like to acknowledge their appreciation for the assistance of Selena J. Linde and Todd M. Hinnen, partners at Perkins Coie LLP, in the preparation of this article, although the views expressed are those of the authors.

NOTES

1 *See, e.g.,* David E. Sanger, "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack," *N.Y. Times*, Aug. 31, 2014, available at *www.nytimes.com/2014/09/01/world/europe/nato-set-to-ratify-pledge-on-joint-defense-in-case-of-major-cyberattack.html?_r=0*.

2 "OCIE Cybersecurity Initiative" (*OCIE National Risk Alert*, Vol. 4, Issue 2), Apr. 15, 2014, available at *www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf*.

3 Reference in this article to primary service providers refers to a fund's adviser, administrator, transfer agent, distributor and custodian.

4 *See* Emily Glazer, "J.P. Morgan CEO: Cybersecurity Spending to Double," *Wall St. J.,* Oct. 10, 2014, available at *http://online.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976* (describing the announcement that J.P. Morgan will double its cybersecurity spending over the next five years following an attack by external hackers that compromised data belonging to 76 million households and 7 million businesses); and Andrea Peterson, "When Cybersecurity Threats Come from the Inside," *Washington Post*, Oct. 8, 2014, available at *www.washingtonpost.com/blogs/the-switch/wp/2014/10/08/when-cybersecurity-threats-come-from-the-inside/* (describing AT&T's acknowledgement that an employee had obtained unauthorized access to personal data belonging to customers for what appeared to be fraudulent purposes). The New York Times has also reported that "President Obama and his top national security advisers began receiving periodic briefings on the huge cyberattack at JPMorgan Chase and other financial institutions this summer." Michael Corkery, *et al.*, "Obama Had Security Fears on JPMorgan Data Breach," *N.Y. Times*, Oct. 8, 2014, available at *http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/*. It is noteworthy that Fidelity Investments is also reported to have been targeted, *Id.*, and that J.P. Morgan holds many trillions of dollars of mutual fund assets in its custody bank. *See www.jpmorgan.com/pages/jpmorgan/is/products/custody.*

[5] Damages sought by investors and other customers in suits relating to data/privacy breaches "typically include claims of unfair competition, negligence, invasion of privacy, breach of express or implied contract, bailment and violation of consumer protection law." John Black, "Developments in Data Security Breach Liability," 69 *BUS. LAW* 199, 200 (Nov. 2013).

[6] Cybersecurity breaches have the potential to result in violations of the federal securities laws, including, but not limited to, those pertaining to: insider trading, material nonpublic information and disclosure of investment company holdings (Section 10b of the Securities Exchange Act of 1934 and Form N-1A under the Securities Act of 1933); investment company codes of ethics and compliance programs (Rules 17j-1 and 38a-1 under the Investment Company Act of 1940 (the 1940 Act)); the privacy of consumer information (Regulations S-P and S-ID); money laundering (the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001); and adviser codes of ethics and compliance programs (Rules 204A-1 and 206(4)-7 under the Investment Advisers Act of 1940).

[7] *See, e.g.,* the California Data Breach Law (Cal. Civ. Code § 1798.29; 1798.80 *et seq*.), which was amended on September 30, 2014 and requires businesses "to notify any California resident whose unencrypted personal information … was acquired, or reasonably believed to have been acquired, by an unauthorized person" and to offer such individuals free identity theft prevention and mitigation services for at least one year.

[8] Alan Friedman, *et al*., "Thoughts On Cyber Security – Liability, Damages And Insurance," 17 *FINTECH LAW REP.* 1 (Mar./Apr. 2014), available at *www.crai.com/uploadedFiles/Publications/Thoughts-on-cyber-security.pdf.*

[9] According to research performed by the Ponemon Institute, "in the non-malicious breach the discovery was accidental (34 percent) followed by a loss prevention tool such as DLP (16 percent). Malicious breaches were most often discovered through the use of forensic methods and tools (28 percent) and DLP or other loss prevention tools (19 percent). Non-malicious breaches were discovered in an average of 49 days and for malicious breach 80 days." Ponemon Institute, "The Post Breach Boom Study" (Feb. 2013). The average structured query language (SQL) injection breach takes 140 days to discover. Ponemon Institute, "The SQL Injection Threat Study" (Apr. 2014).

[10] *See* Amey Stone, "A Primer on the Mutual-Fund Scandal," *Bloomberg Bus. Wk*. (Sept. 21, 2003), available at *www.businessweek.com/stories/2003-09-21/a-primer-on-the-mutual-fund-scandal.*

[11] Indeed, mutual fund registration statements typically disclose the policy and procedures of the adviser regarding the correction of NAV errors and "as of" trades.

[12] Boards should consider with counsel whether their funds' current prospectuses and other disclosure documents appropriately disclose any possible risks to shareholders with respect to cyberlosses.

[13] A comprehensive chart summarizing state security breach notification laws is available at *https://ruby.perkinscoie.com/images/content/1/0/109834.pdf*.

[14] Penny Crosman, "How this Mutual Fund Giant Stays a Step Ahead of Cyber Crooks," *Am. Banker* (Oct. 17, 2014), available at 2014 WLNR 28858989.

[15] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 2014), at pp. 1-3, available at *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf*.

[16] Panel remarks at SEC Cybersecurity Roundtable (Mar. 26, 2014); *see also* Louis A. Aguilar, "The Commission's Role in Addressing the Growing Cyber-Threat," remarks at SEC Cybersecurity Roundtable (Mar. 26, 2014) (transcript available at *www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184#.VCXIcvldX08)*.

[17] Typically, the confidential data belonging to a mutual fund that passes through its service providers' IT systems will include information regarding (i) portfolio holdings, financial condition, trading strategies and pending transactions, (ii) other proprietary

information regarding the fund's business operations, and (iii) personal information regarding prospective and existing fund shareholders and employees, which may include, among other items, names, social security and tax identification numbers, credit card and other account numbers, identifying credit history and demographic data.

[18] Statement on Standards for Attestation Engagements No. 16 (SSAE16) and Service Organizational Control 1 (SOC1) reports cover a service provider's internal controls, including IT-related controls, relevant to financial reporting. Service Organizational Control 2 (SOC2) and Service Organizational Control 3 (SOC3) reports address a service provider's internal controls, including IT-related controls, relevant to compliance and operational matters, including security, availability, processing integrity, confidentiality and privacy. Independent accounting firms typically conduct SSAE16, SOC1, SOC2 and SOC3 audits and prepare the resulting reports for mutual fund groups. All SOC reports follow the Trust Principles of the American Institute of Certified Public Accountants (the AICPA). SSAE16 reports follow Audit and Attest Standard No. 801 of the AICPA.

[19] Sample questions may include: whether the firm has had any computer or information security incidents during the past several years; whether the firm or its operational systems have been the subject of targeted computer security threats; the average time to discover such computer security incidents; whether the firm has a published information security policy and senior employees directly charged with information security; and whether the firm follows any formal information risk management frameworks or standards or holds applicable information security certifications.

[20] Matt Egan, "Companies Turn to Cyber Insurance as Hacker Threats Mount," *FOXBusiness* (Mar. 20, 2014), available at *www.foxbusiness.com/technology/2014/03/20/companies-turn-to-cyber-insurance-as-hacker-threat-mounts/*.

[21] John Reed Stark, "Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught," 46 *Sec. Reg. & Law Rep*. 770, *reprinted in Bloomberg BNA Sec. Reg. & Law Rep*. (Apr. 21, 2014).

[22] Such standards include, but may not be limited to, those developed by the NIST, the International Organization for Standardization, the Center for Internet Security and the SANS Institute.

[23] At a minimum, the written IT/data security program should establish policies and procedures designed to ensure physical security of network hardware, prevent bad actors from being hired as employees, train employees with respect to IT/data security expectations and ensure that employees who exhibit chronic and/or material failure to comply with the security program will be terminated.

[24] At a minimum, the network security program should incorporate appropriate disaster recovery/business continuity plans and provide for, among any other appropriate measures: encryption protocols covering all fund data flowing through the network; regular network risk assessments; continuous updating of risk management plans; monitoring for unauthorized and otherwise aberrant access to the network and fund data housed therein; maintenance of recording and logging systems for the originating address, user identifier and date and time of all successful and unsuccessful logon attempts to the network; information barriers and/or other segmenting systems that limit access to fund data on a "need to know" basis; multi-factor authentication for network and application user access, and controls to avert both unauthorized escalation of user privileges and lateral movement among network resources; regular inventorying of hardware and software with permitted access to the network; enforcement and regular updating of security and policies regarding mobile devices, including that passwords must be technically strong and changed regularly; processes that prevent users from impermissibly altering network hardware and software; central management and deployment of software updates/patches and anti-virus programs on all registered equipment and devices; protections against distributed denial of service (DDoS)

attacks; regular testing and auditing of all cybersecurity controls; and corrective action and incident response/escalation plans.

[25] Such liabilities may include, without limitation, attorneys' fees, identity protection and/or credit insurance for affected shareholders, and any other services that may be necessary for the funds to comply with applicable laws and/or regulatory actions, prevent injury to shareholders, and avoid all commercial, reputational, and legal risk.

[26] PricewaterhouseCoopers LLC, "Answering Your Cybersecurity Questions: The Need for Continued Action" (Jan. 2014), available at *www.pwc.com/en_US/us/increasing-it effectiveness/publications/assets/answering-your-cybersecurity-questions.pdf.*

[27] "CF Disclosure Guidance: Topic 2, Cybersecurity" (SEC Division of Corporation Finance), Oct. 12, 2011, available at *www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm* (providing interpretive guidance about disclosures related to material cybersecurity matters, including "relevant insurance coverage"); and OCIE, *supra* n.2 (explaining that registered investment advisers and broker/dealers should be prepared to provide OCIE with information regarding whether the firm maintains "insurance that specifically covers losses and expenses attributable to cybersecurity incidents," and if so, the nature of the coverage and "whether the firm has filed any claims, as well as the nature of the resolution of those claims").

[28] Brian E. Finch, "CIOs Spur Revenue Generation Through Smart Cybersecurity," *Wall St. J.,* Sept. 11, 2014, available at *http://blogs.wsj.com/cio/2014/09/11/cios-spur-revenue-generation-through-smart-cybersecurity*.

[29] For example, a third party vendor may manage or host critical applications for a fund. In the event that the vendor experiences a malicious cyberattack (hacker, virus, rogue employee, etc.) the subsequent disruption could cause the fund to lose income if it is unable to access a critical application and conduct business.

[30] Nicole Perloth & Elizabeth A. Harris, "Cyberattack Insurance a Challenge for Business," *N.Y. Times*, June 8, 2014 (*citing* The Ponemon Institute's May 2013 "Cost of Data Breach Study: Global Analysis 1, 5," which estimated that the cost of a data breach in 2013 was $188 per compromised record). *See also* Egan, *supra* n.20 (explaining that cybersecurity insurance premiums can vary significantly, from $2,000 to more than $50,000 per $1 million).

[31] *Id.*

[32] *www.dhs.gov/publication/cybersecurity-insurance*.

[33] *Id.*

[34] DHS NPPD, "Insurance Industry Working Session Readout Report, Insurance for Cyber-Related Critical Infrastructure Loss" (July 2014), available at *www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf*.

[35] *Id.*

[36] Perloth & Harris, *supra* n.30.

[37] Christopher M. Matthews, "Cybersecurity Insurance Picks Up Steam, Study Finds," *Wall St. J.,* Aug, 7, 2013, available at *http://blogs.wsj.com/riskandcompliance/2013/08/07/cybersecurity-insurance-picks-up-steam-study-finds*.

[38] Noah Buhayar, *et al.*, "JPMorgan's Data Breach Reveals Growth Market for Insurers," *Bloomberg*, Oct. 9, 2014, available at *www.bloomberg.com/news/2014-10-09/jpmorgan-s-data-breach-reveals-growth-market-for-insurers.html.*

[39] Stark, *supra* n.21.

[40] Crosman *supra* n.14, quoting the Chief Information Security Officer of Pioneer Investments: "Every good chief security officer and every risk manager worth his salt will understand completely what constitutes an annualized loss expectancy [for a mutual fund group]. That's just a ballpark estimate based on past events, based on landscape, based on what's happening with competitors and things like that. That's what you can expect to lose, but when you take that into the overall equation of what you're expecting to gain by executing on your road map, it's simple numbers. Especially when you can unequivocally demonstrate that particular events that happened did not cause disruption … If you start with a company that has

cybersecurity insurance, you can take the worst-case deductible out of that. Say a company has a $250,000 deductible for an incident breach that would result in $10 million worth of loss. That's a set number you can include in the equation. Especially in financial services, executives understand money very well, but technology, if it's not enabling the business directly, you've got to show at least the indirect method [of] how it's enabling the business."

41 NIST, *supra* n.15.