MUTUAL FUND DIRECTORS FORUM

The FORUM *for* FUND INDEPENDENT DIRECTORS

Report of the
Mutual Fund Directors Forum

Board Oversight of Cybersecurity

November 2015

TABLE OF CONTENTS

I. Introduction 1

II. Understanding the Context of Cybersecurity Risk 3

An outline provided by the adviser of the key systems used by the fund can assist the board in gaining a familiarity with the fund's technological framework. 3

Boards also may find summary information about the fund's key service providers useful in their oversight of cybersecurity issues. 3

As part of developing an awareness of the technological framework, boards may also wish to receive summary information on the fund's sensitive data and how it is stored. 4

Boards should have a basic awareness of the ongoing threats to the technology infrastructure on which the fund relies and risks to the integrity of critical fund data. 4

III. Overseeing Cybersecurity Risk Management 5

The board should determine how to structure its oversight of cybersecurity risk management. 5

A discussion with the adviser can help boards learn how management protects its technology framework from these threats. 5

Boards should be familiar with how management oversees other third-party service providers. 6

Establishing a reporting and notification policy in case of cybersecurity events will provide boards with information necessary to provide effective oversight. 6

The Board may wish to review any plan the adviser has developed to respond to a cybersecurity event. 7

The fund CCO and other personnel can be helpful to the board in cybersecurity oversight. 8

A disclosure review process that includes cybersecurity can help the board determine whether existing disclosure regarding cybersecurity risk is adequate. 8

A management review of current contracts can help the board appreciate how potential losses may be covered under existing contracts and insurance policies. 9

IV. Appendix 11

V. Notes 13

Introduction

Mutual fund boards have long had a role in overseeing the manner in which fund management and others identify, monitor, and mitigate the risks that their funds face. One key risk category for mutual funds is operational risk.[1] As we noted in our 2010 Report on risk oversight, "operational risk is the risk that issues will arise or errors or omissions will occur in the ordinary course of business that . . . will adversely affect the business enterprise" resulting in "the business not be[ing] able to operate, whether in the ordinary course of business or during a disaster."[2]

Today, virtually every aspect of a fund's operations relies in some way on technology, and thus the risks posed by that technology have become a fundamental aspect of the operational risk faced by funds. In short, a failure of technology will translate to difficulty conducting fund business, whether that means the fund is unable to process shareholder transactions, manage sensitive shareholder and portfolio data, properly value its portfolio and compute its net asset value, or ensure safe and accurate custody of the securities it owns, to name a few critical functions.

Technology can fail for numerous reasons, including issues with hardware, programming mistakes, or corrupted data.[3] But of late, a new risk has become prominent—the risk that the technological framework on which the fund relies will be attacked by someone with malicious intent. Funds, management companies, and other fund service providers are thus devoting ever-increasing resources to "cybersecurity," the primary means by which they protect themselves from this risk.

While many of the recent publicly-acknowledged attacks have focused on retailers and banks, mutual funds remain a potential target due to sensitive investor information, fund trading records, and other proprietary information. As attacks in other industries have demonstrated, cyber attacks can take numerous forms. Gaining access to a fund's systems, for example, can be as simple as tricking employees into turning over credentials, either through broad-based communications (known as "phishing") or through elaborate and personal communications (known as "spear phishing"). Alternatively, outsiders may try to use "vulnerabilities," or weaknesses, in systems to gain unauthorized access. To simply cause a disruption, attackers may utilize a distributed network of compromised computers to overwhelm the target system with useless requests in a "Distributed Denial of Service" (DDoS) attack, causing the system to be unable to meet the requests of legitimate traffic. Destructive attacks may even come from within, initiated by disgruntled employees. Moreover, the modes of attack continue to evolve.

Efforts to bolster fund operations against attack and to improve the protection of sensitive information have, not surprisingly, become areas of interest for regulators. The SEC's Examination Priorities for the past two years have identified cybersecurity issues as an area of focus.[4] At the Forum's 2014 Policy Conference, SEC Commissioner Luis Aguilar noted that "[c]ybersecurity is an area that will only grow in importance, and fund boards need to get out in front of the problem to help prevent and mitigate investor harm."[5]

In April 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) announced that it would conduct a sweep focused on understanding how broker-dealers and investment advisers address cybersecurity.[6] In February 2015, it released a summary of findings from the first round of examinations.[7] While the vast majority of firms had taken some steps to implement a cybersecurity program, the summary revealed gaps in preparation. For example, a small minority of firms had yet to even adopt a written information security policy.[8] In September 2015, OCIE released an additional risk alert and announced a second round of examinations, which it noted would "involve more testing to assess implementation of firm procedures and controls."[9]

The associated risk alerts and sample requests provide a starting point for any organization as it considers cybersecurity readiness. Guidance from the SEC's Division of Investment Management following the initial sweep report acknowledged "that it is not possible for a fund or adviser to anticipate and prevent every cyber attack," but that "[a]ppropriate planning to address cybersecurity and a rapid response capability may, nevertheless, assist funds and advisers in mitigating the impact of any such attacks and any related effects on fund investors and advisory clients, as well as complying with the federal securities laws."[10]

Given the risks posed by cyber attacks and the increased attention and resources being devoted to this issue, fund boards have become increasingly involved in overseeing management's cybersecurity activities. The Investment Company Act and rules promulgated thereunder do not explicitly charge directors with cybersecurity oversight. Nonetheless, as a result of the board's obligation to approve the fund's policies and procedures along with the policies and procedures of certain service providers under Rule 38a-1,[11] boards should have a sense of how these service providers are preparing for and would respond to a cybersecurity incident. In addition to the service providers covered under Rule 38a-1, others, such as custodians, are critical to the day-to-day functioning of the fund, and therefore boards have an interest in learning how these entities have prepared for a cybersecurity incident.

Every fund is different; therefore, a board's cybersecurity oversight will vary based on factors including fund size, number of funds, and the fund's service providers, to name a few. This report[12] is designed to aid fund directors by outlining some of the risks in this area as well as providing some examples of how boards may wish to address their ongoing oversight responsibilities.

Understanding the Context of Cybersecurity Risk

As a starting point, boards can properly orient their oversight by keeping a focus on the risk to and potential impact on fund shareholders as they approach cybersecurity. Risk in this area springs from numerous sources and is constantly changing. Boards can increase the effectiveness of their cybersecurity oversight by adopting a risk-based approach that focuses on the largest and most impactful sources of risk for fund shareholders. Thus, boards may want to begin by understanding the context of cybersecurity risk.

While funds have long relied upon technology, the risks of hacking, cyber attacks, and other related technological risks are relatively new. Further, unlike many areas of board oversight which either explicitly or implicitly emanate from the Investment Company Act, cybersecurity risk is not specific to the fund industry. As a result, boards may not have focused extensively on overseeing these risks and emerging threats until recently. However, the current regulatory and threat environment have made it advisable for boards to develop such a focus. Below, we outline a number of areas where boards may benefit from additional familiarity.

An outline provided by the adviser of the key systems used by the fund can assist the board in gaining a familiarity with the fund's technological framework.

As an initial step, directors should have some awareness of the technology upon which the fund relies; however, directors are not expected to have a detailed understanding of that technology. Asking the fund's adviser to identify key systems and which of those systems are owned and/or managed by the adviser and which parts are owned and/or managed by third parties can provide a helpful foundation for boards to put the technological framework servicing the fund into perspective. As part of this process, boards also may wish to ask management to identify what it believes are the most critical aspects of its technological framework used to support the fund (e.g., striking the NAV, processing shareholder transactions, processing portfolio trades, and so on).

Boards also may find summary information about the fund's key service providers useful in their oversight of cybersecurity issues.

A fund depends on the technology of other service providers as much as it depends on the technology infrastructure of its own adviser. For example, the computer systems of the fund's custodian, underwriter, transfer agent, pricing services, sub-advisers, and others may be crucial to the fund's day-to-day operations.[13]

While information about the technology employed by these service providers may be somewhat more difficult to obtain than information about the adviser's technology infrastructure,[14] the information is likely to be important for management to understand the cybersecurity risks that the fund faces. In less detailed form, this information may also be helpful for the board. As a result, the board may wish to request, through management, summary information regarding the systems and technology of key service providers.[15]

As part of developing an awareness of the technological framework, boards may also wish to receive summary information on the fund's sensitive data and how it is stored.

Essential data in a fund complex can take many forms—ranging from information about a fund's holdings to information about its investment strategy to information about the investors in a fund and the transactions in which they engage with the fund. Much of this information is sensitive or proprietary, and its ongoing integrity is crucial to numerous fund operations.

As a result, boards may want information on the types of sensitive data for which the fund is responsible, where that data resides, and who is responsible for its integrity and security. Depending on the fund's particular characteristics, this type of information could be voluminous, and boards may wish to request that this information be presented to the board as a high-level overview.[16] Boards may also want to request that the summary focus on the fund's largest service providers and the service providers with access to the most sensitive or greatest volume of data.

Boards should have a basic awareness of the ongoing threats to the technology infrastructure on which the fund relies and risks to the integrity of critical fund data.

As with other risk areas, directors are not responsible for developing a plan to deal with cybersecurity risk or otherwise protecting the fund's assets, data, and technology infrastructure from hackers or other threats. However, providing effective oversight requires that directors gain an overall familiarity with the sources of risk. While the implementation and systems involved in cybersecurity can be difficult to master for individuals outside of the information-technology sector, a basic awareness of the threats can aid directors in their oversight role.

As in many other areas of risk management oversight, education is key. If management has sufficient expertise in-house, the board may want to request a presentation from management's Chief Information Security Officer (or analogue). This individual is responsible for overseeing a program to protect a company's data and information technology systems. Organizations without a Chief Information Security Officer may assign this responsibility to another executive, such as a Chief Risk Officer, Chief Security Officer, Chief Information Officer, or even the Chief Executive Officer.

Such a dialogue with management can be helpful in becoming familiar with the general threat landscape and the specific threats that the fund has faced or is likely to face in the future. In some cases, an outside point of view can also be helpful; boards may therefore consider soliciting training from outside experts and attending director-oriented educational events provided by industry groups. In the current environment, threats are numerous and constantly evolving, and as a result, boards may want to continue cybersecurity education on a periodic basis in an effort to keep current on risks facing the fund.

Overseeing Cybersecurity Risk Management

Familiarity with the systems on which the fund relies for its day-to-day functioning provides a useful foundation for overseeing management's ongoing process of identifying and mitigating the cybersecurity risks that the fund faces. Outlined below are some of the ways in which the fund's board might address its ongoing oversight responsibilities. In the appendix to this document, we provide additional questions boards may find helpful to have the adviser answer for the board's consideration. As the board considers the process that will be most effective in its particular circumstances, it should take care that its actions are properly documented, with appropriate discussion in meeting minutes.

The board should determine how to structure its oversight of cybersecurity risk management.

In order to operate efficiently and effectively, the board should consider how to best organize its oversight of cybersecurity. The board may want to consider issues such as how it wishes to receive ongoing updates regarding the implementation and effectiveness of the cybersecurity program, timely notification of cyber events, documentation of the program in minutes and policies and procedures, and the best use of the fund's chief compliance officer (CCO).

Where the duties of overseeing cybersecurity should rest at the board level is another consideration for fund boards. The board may determine that the issue best fits with the compliance, audit, or risk committee, or perhaps with the board as a whole. However, even if cybersecurity oversight primarily rests with a committee, a basic awareness of the threats facing the fund and the steps that management and key service providers are taking to address those threats is helpful to each director.

A discussion with the adviser can help boards learn how management protects its technology framework from these threats.

The board's familiarity with management's approach to cybersecurity is important for oversight because the adviser will play an important role in due diligence and implementation of the cybersecurity program. No organization can eliminate cybersecurity risk; however, management can and should seek to identify and mitigate risks.

A starting point to this discussion may entail a conversation with management relating to its overall approach and attitude regarding cybersecurity. The discussion can include the adviser's organizational structure relating to cybersecurity and provide boards with important information such as the identification of the individual at the adviser who is ultimately responsible for the cybersecurity program. A discussion regarding the reporting structure for the responsible individual can help the board evaluate the adviser's commitment to cybersecurity. Additionally, an understanding of the reporting structure can inform where questions should be directed as they arise.

Boards may also want to inquire into the level of resources that management has devoted to the area, including training and continuing education for those with cybersecurity responsibility, testing and training for all employees,[17] and tools to protect critical infrastructure and detect unauthorized activity. If available, comparative information regarding the budgets of similar organizations may be useful.

The discussion with the adviser can include whether management has adapted broad industry guidance (such as the framework published by the National Institutes for Science and Technology)[18] to its ongoing approach to cybersecurity. Additionally, boards may want to request that management complete the sample requests included with the April 2014 and September 2015 OCIE Risk Alerts and share the results with the board. A review of this exercise can provide an excellent overview of management's program. Boards may also find it helpful to leverage existing resources, such as by reviewing the adviser's Service Organization Control (SOC) reports or the results of any other relevant third-party testing.

Boards should be familiar with how management oversees other third-party service providers.

Other fund service providers, from sub-advisers to record-keepers to custodians, will each have their own cybersecurity risks and issues. However, service providers require a certain level of access to systems and information in order to perform functions on behalf investors and the fund, and thus cybersecurity risk at a third-party service provider can translate into risk for the fund. Similarly, a disruption to a service provider's operations may mean that the fund will be unable to meet its obligations.

While management leads the oversight and diligence process to identify these risks, information about the adviser's process in this regard can help boards in their oversight responsibilities. As a result, boards may want to request an overview of the adviser's vendor risk management program. An understanding of how the adviser oversees vendors and identifies and classifies related risk can give some level of comfort that management is conducting proper diligence.

Some boards may want to be involved to a degree in this process, particularly in the case of the fund's largest or most important service providers. The same considerations discussed in oversight of management's approach to cybersecurity apply in this context. Rather than receiving voluminous data, boards may find it more helpful for management to prepare a summary of its findings. Given the number of service providers, boards and management may want to take a risk-based approach, focusing on the largest and most important service providers.

As a part of the 15(c) process, boards may consider including detailed cybersecurity queries in the questionnaires sent to service providers. These questions may be developed in conjunction with fund counsel and management.[19] Answers to these questions may assist boards in their oversight, and may also help a board demonstrate to service providers and regulators its commitment to cyber oversight.

For service providers of particular importance, the board may also find it helpful to request direct presentations; indeed, larger service providers will likely be accustomed to responding to this type of request. Though time constraints will prevent boards from conducting these types of meetings with all service providers, presentations from a select few providers may offer additional insight into the approach taken to cybersecurity.

Establishing a reporting and notification policy in case of cybersecurity events will provide boards with information necessary to provide effective oversight.

Establishing an appropriate reporting and notification policy can help boards in their oversight responsibilities by providing comfort that the board will be appropriately informed in case of a cybersecurity incident.[20] This reporting expectation is in addition to any board-requested regular updates from management, which may include information on the changing threat landscape and other non-urgent cybersecurity matters.

For non-routine issues, the board may want to consider developing a clear, written policy detailing its notification and escalation expectations. Given that cybersecurity events at service providers

can impact the fund, the board may want to ask that management discuss with service providers similar notification and escalation procedures. Management may wish to consider whether to negotiate these procedures in the next contract renewal with the provider.

The timeline within which the board may wish to be notified will likely vary based on the severity of the attack and its impact. For example, events with minimal impact to the fund and its operations may not warrant an immediate notification in the manner in which a high impact event may, and low severity events may be discussed at the next scheduled board meeting. However, when meaningful and impactful cybersecurity events occur, prompt notification to the board will assist it in its oversight responsibilities.

The board may also want to specify the manner in which it would like to be notified. For example, a board may request that notifications are filtered through the board chair or other individual director, or through a specific committee, such as the compliance committee.

The Board may wish to review any plan the adviser has developed to respond to a cybersecurity event.

From the adviser's perspective, a prompt response in the event of a cyber attack can help mitigate consequences. Hence, many advisers have included potential responses to a cyber attack or similar event in their business continuity plans. While the board does not directly craft the plan, it may want to provide oversight in this area and familiarize itself with how an adviser has prepared for contingencies. Contemplating potential threat scenarios and developing a corresponding response for each different type of threat can help management create an effective plan. For example, an attack meant to disable a fund will require a different response than an attack meant to steal confidential information. An adviser can be better prepared to deliver a useful response to an attack if it has identified critical systems and key vendors necessary for the ongoing operation of the fund and considered how a failure at these key points would impact the fund.

Plans that identify individuals responsible for leading the fund's response can eliminate uncertainty during a cybersecurity event. In addition to technology and information security staff, it can be helpful to involve individuals from across management's organization in the plan's development. Given the notification requirements of some jurisdictions when consumer data is lost and the potential for legal ramifications, inclusion of fund counsel may be appropriate. Additionally, management's public relations department can help shed light on the best public response in certain situations. Lastly, the plan may identify third-party providers able to assist with a response to a cybersecurity event where necessary, such as data forensics firms or specialized information technology teams.

The board may want to be updated as management creates, updates, and tests the plan. Additionally, a review conducted by management of the operation of the response plan after a cyber attack and corresponding summary provided to the board can provide insight into areas that may need to be adjusted. Management's stance towards preparing for its response to potential threat scenarios and adapting its plan to cyber attacks may also provide a view into how seriously it takes cybersecurity risk.

The fund CCO and other personnel can be helpful to the board in cybersecurity oversight.

As with other areas of risk, the fund's CCO, acting on behalf of the board, can be a useful resource in the oversight of cybersecurity risk. The CCO has an "on the ground" view of the operations of the fund and therefore often provides a unique perspective and first look at emerging issues and can help the board oversee this area.

However, the CCO is unlikely to be a cybersecurity expert. The board may want to consider discussing with the CCO her relationship with management's Chief Information Security Officer or functional equivalent, and her access to relevant cybersecurity information.[21] In some cases, the CCO may find it useful to undergo some cybersecurity education to obtain a familiarity with current issues. Having a basic familiarity with the threats facing the fund and the systems employed by the adviser and other service providers may help the CCO perform her duties more effectively.

Additionally, the board may want to consider developing a relationship with the member of management's staff directly responsible for information security and incorporate periodic reporting from that person into the board's meeting agenda. Larger organizations may have a dedicated Chief Information Security Officer, but for other organizations, the role may be held by another individual. This individual will likely be the most well-versed in the threats facing the fund and an open dialogue may add important perspective and insight for the board.

A disclosure review process that includes cybersecurity can help the board determine whether existing disclosure regarding cybersecurity risk is adequate.

As a risk facing the fund, the board should consider whether and how cybersecurity risk is disclosed.[22] The board should undertake this review carefully, given that directors are deemed to have signed fund registration statements and provisions of the Securities Act of 1933 provide for director liability for omissions or misstatements.[23]

The review can begin with a careful consideration of the specific threats and the potential consequences of an attack. This exercise can help boards, together with fund counsel, evaluate whether the risk to the fund is material and whether the level of disclosure adequately represents the risks faced by the fund. In some instances, the fund's existing disclosures may cover all sources of material risk.

If the board and counsel determine that cybersecurity-specific disclosure is appropriate, the next consideration is where the disclosure should appear. While many funds may choose to disclose the risks in the fund's Statement of Additional Information as opposed to the prospectus, this determination should be made on a fund-by-fund basis considering the materiality of the risk after a full examination of the facts. If the board and counsel determine that disclosure is advisable, a further discussion may be the level of detail necessary.

A management review of current contracts can help the board appreciate how potential losses may be covered under existing contracts and insurance policies.

Losses resulting from a cybersecurity incident can represent a substantial risk to shareholders, and boards should consider carefully how the fund is protected against such a loss. Boards may find it useful to request that management develop a number of "use cases," or cybersecurity scenarios, to help determine coverage gaps in existing insurance policies and uncertainties in the allocation of liability.

Boards may want to request that management conduct a review of current contracts with service providers to determine how the contracts allocate cybersecurity risk and obligations. While some cases of liability may be clearer than others, loss from a cyber attack is possible even in the absence of negligence. Where contracts are silent on cybersecurity issues, boards may wish to discuss with management the possibility of negotiating contract modifications to make obligations and requirements clear before a cyber attack necessitates action. However, some service providers may be resistant to contract modifications or off-cycle contract negotiations; therefore, contract renewal may be a more effective point to pursue such negotiations.

Contracts that parse the financial aspects of a cyber attack and cover issues such as indemnification and allocation of costs can reduce uncertainty. Expenses from an attack can accumulate quickly and include litigation costs, damages, cost of a public relations response, and regulatory fines, to name a few. Given the potential for substantial costs, the board and management may wish to discuss the possibility of adding provisions requiring service providers to carry adequate insurance to cover these types of losses, pending the availability of coverage.

Both management and boards should be cognizant of "fourth-party risk," or risk introduced by a service provider's service provider. Just as a threat at a service provider at the fund is a risk, a threat at a service provider's service provider can be a risk for the fund. The parties may wish to discuss the feasibility of adding contractual provisions that limit the use of shareholder data, including a service provider's ability to make certain data available to its own service providers.

Additionally, boards may want to request presentations from insurance representatives and involve fund counsel to better understand the fund's existing insurance coverage. While specialty insurance covering cyber events is an emerging business line that has not yet fully matured, boards may wish to inquire as to the availability of a policy to bridge any gaps that may exist. Lastly, boards may also want to review the Directors and Officers Liability Insurance with independent counsel to check for exclusions that may result in gaps in coverage.

* * * *

Organizations of all types are facing increased risk of cyber attacks, and mutual funds are no exception. Recent incidents have heightened public and regulator focus on cybersecurity readiness, and fund boards should consider cybersecurity risk in the same way that they consider other areas of operational risk. However, the risks will vary from fund to fund and a one-size-fits-all approach will miss the mark. With an awareness of the threats facing the fund and potential consequences stemming therefrom, boards can provide risk-based cybersecurity oversight.

APPENDIX

Cybersecurity Considerations for Boards

Cybersecurity threats and risks will vary from fund to fund; however, the questions below may provide a helpful starting point for fund boards. The list is not meant to be exhaustive, so additional questions may be appropriate. Similarly, not all questions will apply to all funds. Boards may wish to request that management provide responsive information in the form of an annual memorandum for the board's review.

Adviser/Service Provider Oversight

1. Who is in charge of cybersecurity readiness at the adviser? Does this individual have sufficient and ongoing training to understand cybersecurity issues?
2. What essential fund data exists? Where is it stored? Who has responsibility for it? Who has access to it?
3. What cybersecurity threats or risks does the fund face? How have these threats and risks changed over time?
4. How does management train staff regarding cybersecurity issues and how does it stay up to date with emerging issues?
5. Does the adviser utilize any industry standard cybersecurity frameworks?
6. How does management test its cybersecurity readiness?
7. How has management planned its response to a cybersecurity event?
8. How does the adviser oversee service provider cybersecurity risk?

Board Oversight Structure

9. Which committee, if any, will have primary responsibility for cybersecurity oversight?
10. How often will the board discuss non-urgent issues of cybersecurity oversight and receive reports from management?
11. In which instances does the board want notification of a cybersecurity incident, and how does the board wish to receive such notification?
12. How will the board utilize the CCO to help oversee cybersecurity? Does the CCO have sufficient training to feel comfortable with this task?

Disclosure

13. Is the risk to the fund material?
14. Does the current level of disclosure adequately represent the risks faced by the fund?

Protecting Against and Planning for Loss

15. How is the fund covered by existing insurance policies in the event of a cyber attack?
16. How is liability for loss allocated under existing contracts between the fund and service providers?
17. Would a cybersecurity insurance policy be appropriate for the fund?

NOTES

1 Another key risk is "investment risk," which encompasses all the risks that are inherent in the investment strategies employed by a fund and the types of securities it owns in order to execute those strategies.

2 *See* Mutual Fund Directors Forum, *Risk Principles for Fund Directors* (April 2010) at 8, (available at http://www.mfdf.org/images/uploads/newsroom/Risk_Publication_Electronic.pdf).

3 Prominent recent examples of technology failures include outages at a fund accountant platform and an exchange. While not caused by maliciousintent, these events can give rise to similar considerations to those contemplated in this report.

4 Securities and Exchange Commission, National Exam Program of the Office of Compliance Inspections and Examinations, *Examination Priorities for 2015*, January 13, 2015http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf; Securities and Exchange Commission, National Exam Program of the Office of Compliance Inspections and Examinations, *Examination Priorities for 2014*, January 9, 2014, http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.

5 Commissioner Luis A. Aguilar, Taking an Informed Approach to Issues Facing the Mutual Fund Industry (April 2, 2014), available at http://www.sec.gov/News/Speech/Detail/Speech/1370541390232.

6 Securities and Exchange Commission, National Exam Program of the Office of Compliance Inspections and Examinations, *Risk Alert: OCIE Cybersecurity Initiative*, April 15, 2014 http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf ("2014 Risk Alert").

7 Securities and Exchange Commission, National Exam Program of the Office of Compliance Inspections and Examinations, *Cybersecurity Examination Sweep Summary*, February 3, 2015, http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

8 In reviewing the results, however, it may be worth considering that three-fourths of the advisers included in the sweep had assets under management of less than $900 million and that virtually none of the advisers oversee mutual funds.

9 Securities and Exchange Commission, National Exam Program of the Office of Compliance Inspections and Examinations, *OCIE's 2015 Cybersecurity Examination Initiative*, September 15, 2015, http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination initiative.pdf ("2015 Risk Alert").

10 Securities and Exchange Commission, Division of Investment Management, *Guidance Update: Cybersecurity Guidance*, April 2015, http://www.sec.gov/investment/im-guidance-2015-02.pdf.

11 Regulation S-P, 17 C.F.R. pt. 248 (2009), and Regulation S-ID, 17 CFR Part 248 (2013), are particularly relevant as they relate to the safekeeping of customer information. The SEC recently fined an adviser for violations of Regulation S-P for failing to adopt written policies and procedures regarding the security and confidentiality of client information. In 2013, the sensitive information of more than 100,000 individuals in its care was potentially stolen from a third-party server. I*n the Matter of R.T. Jones Capital Equities Management, Inc.*, File No. 3-16827 (SEC September 22, 2015).

12 This report has been reviewed by the Forum's Steering Committee and approved by the Forum's Board of Directors, although it does not necessarily represent the views of all members in every respect. The Forum's current membership includes over 888 independent directors, representing 124 mutual fund groups. Each member group selects a representative to serve on the Forum's Steering Committee. Nothing contained in this report is intended to serve as legal advice. Each fund board should seek the advice of counsel for issues relating to its individual circumstances.

13 While intermediaries may also represent a significant cybersecurity risk to funds, boards may have less leverage with respect to these entities as compared to other service providers.

14 However, service providers of many types are becoming much more accustomed to receiving and responding to information requests about technology and cybersecurity.

15 Given the volume of information available, the board may find it useful to request that this information be presented in a matrix format, much in the same manner that boards may receive matrices covering other types of risk.

16 As with information regarding the fund's service providers, the board may find the presentation of this information most useful in a matrix format.

17 The 2015 Risk Alert notes that "[s]ome data breaches may result from unintentional employee actions such as a misplaced laptop, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source." As a result, it notes that "[e]xaminers may focus on how training is tailored to specific job functions and how training is designed to encourage responsibleemployee and vendor behavior." Insiders may represent an underappreciated risk and boards may want to consider how management is addressing the issue.

18 NIST, *Cybersecurity Framework,* July 8, 2015, http://www.nist.gov/cyberframework/.

19 Several questions that boards may want to consider can be found in the appendix to this document.

20 Some boards may have existing notification protocols relating to other types of operational issues and may be able to integrate cybersecurity notifications into that existing framework.

21 This information may include previously identified cybersecurity risk areas, management's process for vendor oversight and the results of due diligence exercises, the results of any third-party testing of management's technology infrastructure, and management's action plans and remediation efforts that address potential cyber breaches, among other things.

22 The SEC's Division of Corporation Finance has provided guidance on public companies' cybersecurity disclosure obligations that may help guide this analysis. Securities and Exchange Commission, Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, October 13, 2011, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

23 Section 11(a) of the Securities Act of 1933 provides civil liability where registration statements "contain[] an untrue statement of a material fact or omit[] to state a material fact required to be stated therein or necessary to make the statements therein not misleading." For a more in-depth discussion of potential director liability, see *Cybersecurity: Could Investment Company Directors Be Liable for a Breach?*, available at http://www.klgates.com/files/Publication/572d5da9-e50f-4dc2-89be-b2a631f8969b/Presentation/PublicationAttachment/ 5c9cb8a0-0730-4d20-901c-b8e4e447a4f9/Cybersecurity_Could_Investment_Company_Directors_be_Liable_for_a_Breach.pdf.