The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 22, NO. 2 • FEBRUARY 2015

Cybersecurity: Could Investment Company Directors Be Liable for a Breach?

By Arthur C. Delibert, Marguerite W. Laurent, and Lori L. Schneider

If some evil genius were sitting down to devise ways to torture mutual fund boards of directors, he might have a hard time coming up with a problem more intractable than cybersecurity. Cybersecurity concerns are different than the other hot issues that boards are confronting nowadays, such as valuation policies and intermediary payments, because cybersecurity issues are matters for which board members may not have any intuitive feel from their backgrounds in the business or regulatory worlds, because the problems in the cybersecurity realm are mutating faster than problems in other areas, and because the problems of cybersecurity are imposed largely from outside the organization.

Fund boards are struggling to get a handle on the issues of cybersecurity and, at the same time, wondering whether and under what circumstances they might be held liable for a cybersecurity breach. The federal securities laws do not explicitly address a mutual fund board's oversight responsibilities for cybersecurity, nor have there been any SEC enforcement actions brought against funds or their boards in this area. Cybersecurity has, however, become a topic of considerable attention from the Security and Exchange Commission (SEC) Staff recently, and it does not appear that such attention is likely to subside any time soon. This article looks to general responsibilities under the federal securities laws and state law notions of fiduciary duty to attempt to outline an approach the SEC and the courts might take when evaluating these responsibilities. In considering the existing framework of laws governing board responsibilities, it appears that a careful, thoughtful process by boards that includes regular reports from management and the funds' key service providers about how they identify, manage and mitigate cybersecurity risks, along with a report about how their practices align with industry best practices, could be a strong defense to any claim that boards did not fulfill their duties in this area. Boards should not hesitate to request presentations and regular updates on cybersecurity from their service providers' Chief Information Security Officers, Chief Compliance Officers, and heads of Internal Audit.

A cybersecurity incident can refer to system or technological breaches that allow an unauthorized party to gain access to fund assets, customer personal information, or proprietary trading information, or cause a fund or fund service provider to suffer data corruption or lose operational functionality. Along with the rest of the financial services industry, funds and their service providers have continuously increased the use of technology for many business and operational functions in recent years. Consequently, unless fund service providers take appropriate precautions, funds could be susceptible to operational risks from cybersecurity incidents.

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

Many large organizations have been recent targets of cybersecurity breaches, and it seems as though the occurrence of these incidents — or at least the public reporting of them — is increasing. These breaches have been highly publicized and costly to remediate and have caused immeasurable reputational damage to the companies. The nature of the reports of cybersecurity breaches, and statements from experts in the field, give rise to a discomforting sense that no matter how extensive a firm's cyber protections may be, they may not be enough — that it is not a question of *if*, but *when* a firm will be faced with a cyber intrusion. Consequently, it is not enough for an organization to try to bar the doors against an attack; prudent planning in this area also requires a robust plan for responding when an attack does occur.

Cybersecurity recently has been an area of intense focus for the SEC. SEC Commissioner Luis Aguilar began the SEC's Cybersecurity Roundtable on March 26, 2014, by stating that "[i]n recent months, cybersecurity has become a top concern to American companies, regulators, and law enforcement agencies. This is in part because of the mounting evidence that the constant threat of cyber-attack is real, lasting, and cannot be ignored." In January 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) identified "technology" as one of its "National Exam Program (NEP) Wide" initiatives. Specifically, OCIE noted that the NEP "will continue to examine governance and supervision of information technology systems, operational capability, market access, information security, and preparedness to respond to sudden malfunctions and system outages." Similarly, FINRA announced that cybersecurity would be one of its examination priorities and that its primary focus is the integrity of firms' policies, procedures and controls to protect sensitive customer data.

On April 15, 2014, OCIE released a Risk Alert describing its initiative to assess the securities industry's cybersecurity preparedness and to collect information about recent cybersecurity incidents. The Risk Alert noted that OCIE would be conducting examinations of more than 50 investment advisers and broker-dealers to review cybersecurity matters. The Risk Alert included a sample information and document request letter that could be used in the sweep examination. The sample request asks for, among other things, information relating to the identification of risks and cybersecurity governance, protection of firm networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, and detection of unauthorized activity. Although the sample request is broad, the Risk Alert specifically notes that "[t]hese factors are not exhaustive, nor will they constitute a safe harbor. Other factors besides those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business."

I. Board Oversight Considerations

Nothing in the Investment Company Act of 1940 (1940 Act) or related rules specifically discusses board oversight of cybersecurity, and there have not been any SEC enforcement actions to date against a mutual fund or its board in this area. Therefore, the SEC or a court may look to general responsibilities under the federal securities laws, as well as state law notions of fiduciary duty, for these purposes.

A. Rule 38a-1 under the 1940 Act

Rule 38a-1 under the 1940 Act requires that a fund's board, including a majority of its independent directors, approve the compliance policies and procedures of the fund and the fund's investment adviser, principal underwriter, administrator and transfer agent (each, a Service Provider) on the basis of "a finding by the board that the policies and procedures are reasonably designed to prevent violation of the Federal Securities Laws."[1] Because funds conduct their activities through their Service Providers, the rule specifically requires that a fund's program include policies and procedures that "provide for the oversight of compliance by each investment adviser,

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

principal underwriter, administrator, and transfer agent of the fund." The records and operational capacity on which funds rely generally reside on the IT systems of Service Providers.

The primary aspects of funds' and Service Providers' compliance programs that are relevant to cybersecurity preparedness are:

- Safeguarding client information and records (SEC Regulations S-P and S-ID);
- Safeguarding the integrity of the funds' records and financial reporting systems (1940 Act Rule 30a-3);
- Business continuity plans; and
- Custody of fund assets.[2]

Each of these specific areas is discussed in more detail below.[3]

The SEC's adopting release for Rule 38a-1 stated that a fund board may satisfy its obligations under Rule 38a-1 by reviewing summaries of compliance programs prepared by the Chief Compliance Officer, legal counsel or other persons familiar with the compliance programs and that the summaries "should familiarize directors with the salient features of the programs (including programs of service providers) and provide them with a good understanding of how the compliance programs address particularly significant compliance risks." The adopting release further explains the Commission's view of boards' responsibility:

> In considering whether to approve a fund's or service provider's compliance policies and procedures, boards should consider the nature of the fund's exposure to compliance failures. … Boards should also consider the adequacy of the policies and procedures in light of their recent compliance experiences, which may demonstrate weaknesses in the fund or service provider's compliance programs. We urge Boards to also consider best practices used by other fund complexes and to consult with fund counsel (and independent directors with their counsel), compliance specialists and other experts familiar with compliance practices successfully employed by similar funds or service providers.[4]

The fact that Rule 38a-1 requires boards to approve compliance policies and procedures that are "reasonably designed" to prevent violations suggests that boards' actions in this area would be weighed against a negligence standard of due care. However, because this is a regulatory rule, that standard would likely be applied in the first instance not by the law's proverbial "reasonable person," but rather by a "reasonable regulator," with an agency's regulatory goals in mind and an expectation that boards be aware of the SEC's emphasis in the area of cybersecurity. To the extent the SEC views the compliance procedures as inadequate, it may seek to hold fund directors accountable for a violation of Rule 38a-1.[5]

Rule 38a-1, by its terms, operates largely through a fund group's Chief Compliance Officer (CCO), who may not be the best point of contact in the highly technical area of cybersecurity. The CCO, however, may wish to make sure that there is a compliance structure around cybersecurity and that it is properly implemented. It is important to note, however, that compliance rules cannot ensure that the overall cybersecurity program remains on the cutting edge, which is important if the program is to be effective. Therefore, many fund boards receive regular reports from the management company's Chief Information Security Officer (CISO) or someone in a similar position who is responsible for the overall implementation and development of a fund firm's cybersecurity program.

We discuss below the areas of a fund's or Service Provider's compliance program that appear most relevant to cybersecurity preparedness.

1. Privacy and Regulations S-P and S-ID

The SEC adopted Regulation S-P pursuant to Title V of the Gramm-Leach-Bliley Act, which

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

governs the disclosure of nonpublic personal information and limits the instances in which an investment adviser, broker, dealer, or investment company (SEC-regulated financial institution) may disclose nonpublic personal information about a customer to nonaffiliated third parties.[6] Regulation S-P requires that the policies and procedures:

- address administrative, technical, and physical safeguards for the protection of such information;
- be reasonably designed to insure the security and confidentiality of nonpublic personal information;
- protect against any anticipated threats or hazards to the security or integrity of nonpublic personal information; and
- protect against any unauthorized access to or use of nonpublic personal information that could result in substantial harm or inconvenience to any customer.

Regulation S-P provides examples defining who is or is not a "customer," whose records would be within the ambit of the rule. For investment companies, the definitions in the rule state that a customer relationship is established when an individual "purchases shares you have issued (and the consumer is the record owner of the shares)." Therefore, an individual who purchases fund shares through a broker-dealer and does not have direct contact with the fund (because the broker-dealer is the record holder of fund shares "for the benefit of" the individual) is not a ***fund*** customer under Regulation S-P. Coupled with the fact that Rule 38a-1 specifically reaches the compliance policies and procedures of a fund's principal underwriter, but not those of third-party intermediaries that make fund shares available, this means that fund boards are not responsible under Rule 38a-1 for approving the Regulation S-P compliance policies and procedures of those third-party intermediaries. However, a fund group's principal underwriter may have some accounts in the names of individual shareholders, to which Regulation S-P would apply.

The SEC has brought several enforcement actions over the last several years under Regulation S-P against investment advisory and broker-dealer firms following cybersecurity incidents. These actions typically have involved what the SEC believes to be egregious violations, such as not having cybersecurity protocols that the SEC views as fundamental, having policies that merely restate the rule, or having no policies at all.[7]

Funds that provide check-writing privileges or permit their account holders to wire money to a third party may be subject to Regulation S-ID, the SEC's Identity Theft Red Flag rules, which governs identity theft protection. In the event of a cybersecurity incident resulting in the theft or other public exposure of account holders' personal information, the SEC could possibly allege that the boards of such funds were responsible under Rule 38a-1 if it believed that the Regulation S-ID compliance procedures were inadequate. Regulation S-ID also may apply to the third-party intermediaries servicing fund shareholders if the intermediaries allow shareholders to make these transfers. Since Rule 38a-1 specifically reaches the compliance policies and procedures of a fund's principal underwriter, but not those of third-party intermediaries that make fund shares available, this means that fund boards are not responsible under Rule 38a-1 for approving the Regulation S-ID compliance policies and procedures of those third-party intermediaries.

2. Integrity of Records and Financial Reporting and Rule 30a-3

Mutual funds and their principal Service Providers each are subject to requirements that they maintain certain books and records either as part of their business or on the funds' behalf.[8] It is not inconceivable that the SEC could read Rule 38a-1 to require a compliance program that is reasonably designed to address the security of these records against cyber attacks. Funds also are subject to

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

Rule 30a-3 under the 1940 Act, which requires an investment company to maintain disclosure controls and procedures[9] and internal control over financial reporting.[10] Notably, under the language of Rule 30a-3, such internal control is to be "effected by" the board, management and others.

Cybersecurity may be an important aspect of financial controls, because a cyber breach could impact the integrity of the records or even be used to cover up a loss or theft of fund assets. Also, where all the accounting is done on computers, a denial of service attack or a scrambling of the records could affect the accuracy of a fund's financial reporting. While cybersecurity clearly was not contemplated by Rule 30a-3 or discussed in the adopting release, it is possible that if a cybersecurity breach occurred that impacted the creation or maintenance of financial records, or somehow affected the accuracy of a fund's financial reporting, the SEC may seek to bring an action against a fund board pursuant to Rule 30a-3 for failure to properly "effect" internal control over financial reporting.

3. Business Continuity

Business continuity plans also are important in the context of cybersecurity. If a Service Provider's computer system is shut down or corrupted by a cybersecurity incident, such as a computer virus or a denial of service attack, the fund's ability to continue its operations could be affected. In relation to business continuity plans, the adopting release to Rule 38a-1 explains that "an adviser's fiduciary obligation to its clients includes the obligation to take steps to protect the clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services." Although the Rule 38a-1 adopting release specifically discusses business continuity in relation to a fund's adviser, fund boards also may want to consider the business continuity plans of the other Service Providers on which the funds are critically dependent. A footnote in the adopting release makes a somewhat oblique reference to this point: "Funds' or their advisers' policies and procedures should address the issues we identified for investment advisers above. In addition, we expect policies and procedures of funds (or fund service providers) to cover certain other critical areas." Moreover, FINRA Rule 4370 specifically requires FINRA members (such as a mutual fund's principal underwriter) to adopt a business continuity plan, designate members of senior management responsible for its implementation and disclose to their customers how the business continuity plan addresses possible future significant business disruption. As a practical matter, boards should never be satisfied with business continuity plans that exist only on paper. They should ask whether live drills have been conducted or whether the plan was used in a real catastrophe, and if so, how the plan fared, what lessons were learned and what adjustments were made as a result.

4. Custody of Fund Assets

Section 17(f) of the 1940 Act requires a fund to maintain its securities and other investments with certain types of custodians under conditions designed to assure the safety of the fund's assets. In the event there is a cybersecurity breach at a fund's custodian, the actual assets of the fund could be at risk. The custodian also would have information on the securities that are bought and sold by a fund, so presumably a hacker could gain real-time access to the trading activity of the fund. Thus, fund boards may want to consider hearing from the fund custodians about their cybersecurity protocols and procedures.

There is always a concern when dealing with regulatory enforcement agencies that events will be judged in hindsight, that the fact a breach occurred will be taken as conclusive proof that the policies and procedures were inadequate. In the field of cybersecurity, this concern has to be tempered by recognition that it likely is impossible to ensure complete protection from cyber attacks. Rule 38a-1 requires only that a fund and its Service Providers have policies and procedures that are "reasonably" sufficient to prevent violations. Rule 30a-3(d) (set forth in

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

note 9) uses the word "reasonable" four times to define the scope of what is required. That is, the rule does not require absolute assurance against a breach of internal controls, and the fact of a breach is not, by itself, proof that the rule was violated.

B. Board Oversight of Risk Management

While primary responsibility for risk management in most fund organizations rests with fund management, fund boards generally assert some responsibility for overseeing these risk management processes. In 2009, the SEC adopted a requirement that mandates that mutual funds disclose in their Statements of Additional Information (SAIs) "the extent of the board's role in the risk oversight of the fund, such as how the board administers its oversight function," be it through the whole board, a separate risk committee, or the audit committee. As a result, many funds' SAIs currently discuss the boards' oversight of risk management in areas such as investment risk, counterparty risk, valuation risk, reputational risk, risk of operational failure or lack of business continuity, and legal, compliance and regulatory risk.

Commissioner Aguilar, speaking at the "Cyber Risks and the Boardroom" Conference on June 10, 2014, explained his views[11] on a corporate board's oversight role with respect to cyber-risk:

> Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk — and there can be little doubt that cyber-risk also must be considered as part of a board's overall risk oversight. …
>
> Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. [emphasis added; footnotes omitted]

Thus, it is clear that at least one Commissioner believes that fund boards have an oversight obligation to see that management understands its risk management obligations in the cybersecurity arena, takes them seriously, and has a program that is up to the task. Note, however, that the role Commissioner Aguilar describes for directors is *oversight* of risk management, not risk management itself. As in other areas, boards are not expected to be technology experts or to micro-manage corporate processes — although Commissioner Aguilar's uses of the word "ensure" in his prepared remarks suggest that he may see boards as having a heightened obligation in this area. Nonetheless, the parameters of such a heightened obligation would be difficult to define, and all the more so because this is an area in which no one can "ensure" the adequacy of protection. Whatever is the legal standard for cybersecurity, it should not be one of "ensuring" the adequacy of the security efforts.

C. Fiduciary Duties under State Law

In considering boards' responsibilities for overseeing the cybersecurity preparedness of Service Providers, it is important to consider also the state law standards that would apply to a board's actions. Fund directors are subject to fiduciary duties arising from state laws applicable to corporations or statutory trusts and general common law fiduciary principles. These are the duty of care and the duty of loyalty. Directors are required to perform these duties in good faith and in a manner they reasonably believe to be in the best interests of their funds. In order to satisfy the duty of care, when making a business determination, a director must endeavor to obtain all material information and advice reasonably

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

available in order to evaluate and determine that a proposed course of action is in the best interests of the fund (although, of course, circumstances often dictate that boards must make decisions on less than full information). The duty of loyalty generally requires that a director refrain from engaging in activities that would take advantage of the fund or in matters in which the director has a personal interest contrary to that of the fund. As a general principle, if a court reviewing a board decision determines that the board acted in good faith and in accordance with its fiduciary duties and reached a reasonable decision, the court will not substitute its judgment for that of the board, absent special circumstances.

As a subset of the duty of loyalty, the Delaware courts recognize a duty of board members to monitor corporate affairs with an eye toward preventing harm to the company.[12] Since this is a common law principal and not a statutory provision, a court might extend it to the trustees of a Delaware statutory trust in an appropriate case. There do not appear to be any cases where this duty was applied to a statutory trust board, but there are many Delaware corporate law cases where it was applied to a corporate board. Although known as the *Caremark* standard for the case in which the duty was first set forth, the standard was subsequently refined by the Delaware Supreme Court in *Stone v. Ritter*.[13] In *Stone*, the court established a two-part test for determining a board's liability under the duty to monitor. A board may be liable if it fails to implement any corporate reporting or information system or controls or if, after implementing such systems or controls, it consciously fails to monitor or oversee the corporation.[14]

The *Stone* decision also noted that "imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations," thereby requiring a showing of scienter to prove a breach of the duty to monitor. In the Delaware courts, this standard has been read narrowly, to require actual or constructive knowledge by the board that in failing to establish a monitoring system, or in failing to heed the information coming from the monitoring system, its inaction would harm the corporation. (Constructive knowledge is knowledge that would have been gained with the application of reasonable diligence.) When the Delaware standard has been considered in the federal courts, however, at least some of those courts have imported from Rule 10b-5 cases the notion that recklessness may amount to scienter.[15]

The standard of trustee conduct under the *Caremark* line of cases is thus fairly low, and it seems likely that a board fulfilling its obligations under Rule 38a-1 would also fulfill the *Caremark* standard. However, several important questions do emerge regarding the *Caremark* standard. First, there is a very loud and steady drumbeat coming from the SEC, the news media and elsewhere about the risk of cybersecurity breaches. This drumbeat could be used to argue that a board was reckless in not at least attempting to ensure that management had an adequate framework for considering cybersecurity risks and a robust program for addressing them. Second, *Caremark* could create a basis for personal liability in a private action by shareholders. There are very few provisions of the 1940 Act that allow a private right of action,[16] and Rule 38a-1 does not appear to create a new one. Thus, the *Caremark* line of cases does potentially create risks to boards that do not exist in connection with Rule 38a-1 or Rule 30a-3 alone.[17]

In this regard, boards may want to consider whether there are areas of material cybersecurity risk to their funds that are not subsumed under the rules-based approach of Rule 38a-1. Note, however, that *Caremark* involved the alleged failure to monitor adequately for violations of the law. In two recent cases, the Delaware Chancery Court rejected claims attempting to broaden *Caremark* to impose on corporate directors liability for losses that were not based on the companies' violation of specific legal requirements.[18] The plaintiffs in the two recent cases had argued that in the run-up to the 2008 financial crisis, the boards had failed to prevent their companies from taking undue business risk, but it was risk of

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

the very sort that is essential to their efforts to earn a return. The court declined to impose on the boards a *Caremark* type of obligation to monitor for that type of risk, saying that it conflicted with long-standing doctrine about what lies within the ambit of business judgment and the discretion granted directors that allows them to take risks with the intention, whether ultimately successful or not, of maximizing shareholder value in the long term. Given that the only way for a business to protect itself completely from the risks of a cybersecurity incident is to avoid altogether the use of computers and the internet – a practical impossibility in today's world of financial services – it seems likely that courts will find that the acceptance of some degree of cybersecurity risk is a reasonable business decision, and a cybersecurity incident resulting in loss to the fund is not *per se* grounds for liability.

II. Additional Legal Considerations for Fund Boards

A. Insurance Options

The cybersecurity insurance market is evolving as experience with real-life cybersecurity incidents increases. Some older policies may be interpreted to cover cybersecurity incidents if the policies do not expressly exclude it. However, insurers are now certainly aware of the uncertain size and scope of the risks relating to cybersecurity breaches, and they are attempting to define the limits of such coverage more explicitly. Because funds' fidelity bond and D&O/E&O policies are generally "claims made" policies — that is, they cover claims made at the time the policy is in effect, even if they stem from events that happened in earlier periods — funds likely would have to look to current or future policies for any such coverage.

Fund boards should ask management to evaluate the firm's coverage under current policies (both the fidelity bond and D&O/E&O insurance) and the options for specialty cyber insurance available in the market. One challenge is determining adequate premiums and coverage thresholds for cybersecurity insurance because it is a developing area and the potential risk associated with cybersecurity incidents is not yet fully known and may never be known. Another challenge that is especially important to the fund business is determining exactly where the liability would fall and whose insurance would cover it. Since the data and operating systems that are important to mutual funds reside on the systems of various outside Service Providers and not on systems owned or maintained by the funds, one important point to consider is whether and to what extent cybersecurity insurance purchased by the fund would protect funds for breaches of systems that are not owned or maintained by the funds. And if a fund suffers damages because of a breach that occurs on the system of an outside Service Provider and the fund's insurer disclaims responsibility, is that Service Provider contractually required to reimburse the fund? Service Providers also are becoming more aware of the risks of cybersecurity incidents, and they are reluctant to make any contractual representations about the security of their systems.

B. Registration Statement Disclosure

In October 2011, the SEC's Division of Corporation Finance released guidance on cybersecurity disclosure for public companies.[19] Since that guidance was released, some fund groups have added to their SAIs disclosure on cybersecurity risks, and many others are currently considering it.

Fund boards may wish to discuss with management the materiality of cyber risk to the funds and receive management's input on the types of specific risks involved. Section 11 of the Securities Act of 1933 imposes individual liability on fund directors for material misstatements or omissions in the funds' registration statement, subject to certain defenses, including the board's "due diligence" as to the material accuracy and completeness of the registration statement.

Forms N-1A and N-2 specifically require an investment company's registration statement to summarize the principal risks of investing in the fund,

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

including the risks to which the fund's portfolio as a whole is subject and the circumstances reasonably likely to affect adversely the fund's net asset value, yield, and total return. This is generally understood to mean investment risk, but it could conceivably be read as including material operational risks, including the risk of a cybersecurity incident. These Form requirements, along with the materiality of potential cybersecurity risks, should be evaluated in considering the appropriateness of cybersecurity risk disclosure in fund registration statements.

III. Potential Risks and Board Considerations

A. What are the Risks and Where Do They Come From?

The potential sources of cybersecurity incidents and the effects of those incidents are significant and wide-ranging. Possible cybersecurity threat entry-points can be either physical or technological, thereby requiring both the security of physical property (for example, keycard access to computer hardware, protection of off-site storage and facilities, or video surveillance) and security of the technology platform (for example, firewalls protecting computer servers, data encryption or double authentication log-in requirements).

There are many different sources of cybersecurity incidents or types of cybersecurity attackers. One potential source of a cybersecurity incident is employees of management or other service providers that could cause a cyber breach either intentionally or unintentionally. Such a breach may result from weak policies and procedures for safeguarding or using technology equipment or mobile devices (for example, weak passwords or computer protection) or illicit employee activities. A systems glitch or error also could cause a cybersecurity incident, either by corrupting data, shutting down the system at a critical time, or opening an avenue for an attacker. Other potential sources of cybersecurity incidents include "hacktivists" or computer hackers promoting a political or social agenda, criminals committing fraud, state-sponsored attackers, or industrial competitors committing espionage.

The potential effects of cybersecurity incidents range significantly. Examples include:

- the loss of fund assets;
- the loss or theft of customer personal data or funds;
- customers or employees being unable to access electronic systems (denial of services);
- loss or theft of proprietary information (such as trading information) or fund data;
- physical damage to a computer or network system;
- reputational damage and the associated costs of managing an issue from a public relations point of view;
- remediation costs, including liability for stolen assets, costs associated with system repairs, costs associated with providing affected consumers notice of a breach and the costs of fraud monitoring on credit reports.[20]

Any of these results could have a substantial impact on a fund. For example, if a cybersecurity incident results in a denial of service, fund shareholders could lose electronic access to their accounts for an unknown period of time, and employees could be unable to access electronic systems to perform critical duties for the fund, such as trading, NAV calculation, shareholder accounting or fulfillment of fund share purchases and redemptions. As another example, if a cybersecurity incident resulted in the undetected theft of proprietary fund information, an attacker could use a fund's trade blotter to front-run the fund.[21] The risk of potential reputational damage associated with cybersecurity incidents may also be significant.

B. Third-Party Service Provider Cybersecurity Activities

Fund boards may want to consider whether they have an adequate understanding of the potential

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

cybersecurity threats specifically presented by their funds' third-party service providers, including the transfer agent and custodian. A broader list of third-party service providers may include financial printers, electronic board material platforms, fund pricing services, and independent accounting firms or legal counsel.

Any party that has access to fund data or fund-related systems, either directly or indirectly, may threaten the fund's cybersecurity. For example, the Target cybersecurity incident that occurred in late 2013 reportedly originated through an HVAC service provider that had access to the Target computer network for efficiency updates. According to news reports, a hacker obtained the login credentials of an employee with the HVAC vendor and gained access to the Target computer network to load "malware" and obtain customer information. This incident was possible since the Target heating and air conditioning system and credit card processing system resided on the same Target computer network and all the hacker needed was a single entry-point into the network to wreak havoc.

Each of the third-party service providers may present very different cybersecurity risks in addition to the risks applicable to all fund service providers. For example, a fund's custodian holds the fund's assets and information on the fund's buy/sell activity; the transfer agent, or a broker-dealer with shareholder omnibus accounts, maintains personal or financial information on the fund's shareholders; and the independent accounting firms have access to the fund's accounting and financial records.

Boards may want to consider whether the management company should evaluate the third-party service providers pursuant to the industry cybersecurity standards identified by the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST).[22] It also may consider whether the management entities request Financial Intermediary Controls and Compliance Assessment (FICCA) framework or Statement on Standards for Attestation Engagements (SSAE) 16 auditor reports from third-party service providers. Third-party service providers may voluntarily engage an auditing firm to perform either a FICCA or SSAE 16 audit. The FICCA framework covers seventeen oversight topics, many of which include questions about information technology controls and procedures. A SSAE 16 audit examines the controls at organizations that provide services to other parties and whose controls are likely to be relevant to other parties' internal control over financial reporting.

IV. What Factors Might Fund Boards Consider in Reviewing the Cybersecurity Preparedness of the Funds' Service Providers?

Given the scope and technical complexities of the field of cybersecurity, the most important thing for fund boards to do first is to establish a clear conceptual framework in which to consider the issues. Such a framework might be organized around the following questions:

(1) What types of data and systems do the fund and its manager seek to protect?
(2) What parameters does the manager use to rate the importance of protecting various items of data or various systems (for example, consequences of data falling into the wrong hands, or consequences of a denial-of-service attack, etc.)?
(3) Using those parameters, how does the manager rate the risks to the various categories of data (for example, which ones are of high, medium or low importance to protect)?
(4) Where are the various types of data stored and on whose computers do the systems reside (for example, at the management company, the custodian, the fund's transfer agent, etc.)?
(5) How does the management company protect the data on its systems?
(6) How does the management company oversee, monitor and interact with the service

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

providers that hold some of these data on their systems, with respect to cybersecurity? What type of diligence is conducted? Are the provisions in the contracts with the service providers on confidentiality, privacy, data security and liability for a cyber breach up to date and sufficient?

(7) To what extent have the service providers' cybersecurity programs been captured in written policies and procedures that set forth specific functions, identify the individuals charged with carrying them out and require regular monitoring and reporting?

(8) What structure does the manager have in place to carry out and oversee these functions (for example, is there a CISO, what authority does he/she have, to whom does he/she report, is there an internal committee that works with the CISO, what are the relative roles of the CISO, the CCO, Internal Audit and Operational Risk, and how do they coordinate, etc.)? Is the budget allocated to address cybersecurity adequate and appropriate?

(9) What industry "standards" or best practices exist, and how does the management company measure up against them? How do the other service providers measure up against those standards?[23]

(10) Has the management company received any regulatory or client feedback on its cybersecurity efforts, and if so, what was said? Have the management company and the service providers reviewed the SEC sample sweep letter on cybersecurity, and how prepared are they to respond to such a request if the SEC Staff were to initiate an exam?

(11) What type of regular employee training and testing of the systems and protections are conducted by the management company and other service providers? Are there 'mock' attacks with no advance warning to see how employees perform and whether the system is effective?

(12) Do the management company and the service providers have response plans in place in the event a cybersecurity incident occurs?

(13) Should the board retain a consultant to assist in evaluating management's program?

(14) In the event of a cyber breach, do current insurance policies (such as the fidelity bond or D&O/E&O policies) cover any losses? Would the service providers' insurance cover any losses resulting from a breach of their systems that affects the funds? If not, should 'gap' coverage be considered?

Cybersecurity requires a high degree of vigilance on a continuous basis by the parties charged with managing the systems used to process and store fund-related information. At the same time, there should be written policies and procedures in the areas where it makes sense. The nature of the cybersecurity problem is such that fund directors will never be in a position to *ensure* the security of these systems. Directors can, however, educate themselves about the basic framework in which cybersecurity efforts are carried out, engage in forthright questioning of management and other service providers, explore with those parties any budgetary or personnel constraints on their cybersecurity programs and business continuity plans, and make clear that the directors expect a robust cybersecurity effort from all service providers.

Mr. Delibert and **Ms. Schneider** are partners and **Ms. Laurent** is an associate in the Investment Management practice of K&L Gates LLP. The authors would like to thank Jeffrey Maletta of K&L Gates LLP for his invaluable contributions to the preparation of this article.

NOTES

1 The "Federal Securities Laws" that are referred to in Rule 38a-1 broadly cover: the Securities Act of 1933; the Securities Exchange Act of 1934;

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

the Sarbanes-Oxley Act of 2002; the Investment Company Act of 1940; the Investment Advisers Act of 1940; portions of the Gramm-Leach-Bliley Act governing disclosure of nonpublic personal information; any rules adopted by the SEC under any of these statutes; and the anti-money laundering provisions of the Bank Secrecy Act and any rules adopted thereunder by the SEC or the Department of the Treasury.

[2] Although custodians are not specifically named in Rule 38a-1, fund boards may wish to consider the policies and procedures of their funds' custodians, and the extent to which a failure of their cybersecurity systems could affect the funds. The SEC noted in the adopting release for Rule 38a-1: "In this release, we use the term "service provider" to refer only to a fund's advisers, principal underwriters, administrators, and transfer agents. By limiting the term in this manner, we are not lessening a fund's obligation to consider compliance as part of its decision to employ other entities, such as pricing services, auditors, and custodians." *Final Rule: Compliance Programs of Investment Companies and Investment Advisers*, 1940 Act Release No. 26299, 68 Fed. Reg. 74,714 (adopted Dec. 17, 2003) (Rule 38a-1 Adopting Release) at n.28.

[3] At the Mutual Funds and Investment Management Conference on March 17, 2014, Norm Champ, Director of the Division of Investment Management, stated:

> The Division believes that funds and investment advisers should identify their respective obligations under the federal securities laws and assess the impact of a potential cyber attack on these obligations. For example, IM staff would expect that the compliance policies and procedures of investment advisers and funds would focus on Commission rules, such as Regulations S-P and S-ID, which address data protection and identity theft, including service provider oversight in these areas. Appropriate planning to address cyber security and a rapid response capability may assist funds and investment 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.

[4] Rule 38a-1 Adopting Release, at 74,717.

[5] We note, however, that the two instances in which the SEC has so far brought charges against mutual fund directors under Rule 38a-1 have involved cases where the directors arguably had a special or explicit responsibility. The Morgan Keegan case, *In re Alderman, et al.*, involved fair valuation of portfolio securities, a responsibility given to fund boards by §2(a)(41) of the 1940 Act. *See* In the Matter of J. Kenneth Alderman, CPA, et al., Administrative Proceeding No. 3-15127 (June 13, 2013). The *Northern Lights Trust* case involved an allegation that the board had failed to carry out a specific task set forth in its own compliance policies. *See* In the Matter of Northern Lights Compliance Services, LLC, Administrative Proceeding No. 3-15313 (May 2, 2013). Nevertheless, the SEC Staff continues to raise Rule 38a-1 as a potential basis for charges in examinations and enforcement discussions across a range of issues.

[6] Title V(a) states "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

[7] *See* In the Matter of Commonwealth Equity Services, LLP, Administrative Proceeding No. 3-13631 (Sept. 29, 2009); In the Matter of LPL Financial Corp., Administrative Proceeding No. 3-13181 (Sept. 11, 2008); In the Matter of J.P. Turner & Company, LLC, Administrative Proceeding No. 3-13550 (July 17, 2009).

[8] *See generally* 17 CFR 270.31a-2 and 17 CFR 270.31a-3 applicable to investment companies; 17 CFR 275.204-2 applicable to investment advisers; and 17 CFR 240.17a-3 and 17 CFR 240.17a-4 applicable to broker-dealers.

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

[9] Rule 30a-3 defines "disclosure controls and procedures" as: a fund's controls and other procedures that are designed to ensure that information required to be disclosed by the fund on Form N-CSR and Form N-Q is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms. It further states that disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by a fund in those reports is accumulated and communicated to the investment company's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure. 17 CFR 270.30a-3(c).

[10] Rule 30a-3 defines "internal control over financial reporting" as: a process designed by, or under the supervision of, the registered management investment company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. It also requires that the fund have policies and procedures that (1) pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the investment company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the investment company are being made only in accordance with authorizations of management and directors of the investment company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the investment company's assets that could have a material effect on the financial statements. 17 CFR 270.30a-3(d).

[11] These are Commissioner Aguilar's views which, as he noted in the standard disclaimer he included before providing his remarks: "do not necessarily reflect the views of the U.S. Securities and Exchange Commission, my fellow Commissioners, or members of the staff." As a Commissioner, however, Commissioner Aguilar is one of the people who decide whether an enforcement case is brought and, if it is an administrative case, he is one of the people who would hear an appeal from the Administrative Law Judge's decision.

[12] Since many investment companies are organized as statutory business trusts under Delaware law, this article focuses on the fiduciary duties articulated by the Delaware courts. Different states may have different standards and fund directors should consult counsel regarding the standards that apply to the funds for which they are responsible depending where the funds are organized.

[13] In *In re* Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996), the Delaware Court of Chancery established the duty to monitor as a subset of the duty of care. In *Stone*, however, the Delaware Supreme Court said that it was more consistent with the duty of loyalty. Although the Court did not say this in so many words, this somewhat curious placement of the duty seems to reflect that the Court established a standard of director behavior so low that a violation of the duty could only reflect a near total abandonment by the directors of their duties, thus breaching the duty of loyalty. One consequence of making it a subset of the duty of loyalty is that under the Delaware Corporate Code, a corporate charter cannot exculpate directors from liability for a breach, as it could with respect to the duty of care. It is not entirely clear how this aspect of the duty to monitor would play out in the context of a statutory trust. Stone v. Ritter, 911 A.2d 362 (Del. 2006).

[14] The courts of Maryland, another state under whose laws many investment companies are organized, have not expressly adopted the *Caremark* standard. Maryland defines a director's duty of care by statute.

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

See Maryland Corporations and Associations Code 2-405.1. Maryland courts have held that directors could be liable for conduct amounting to gross negligence. James J. Hanks, *Maryland Corporation Law* § 6.6 (Nov. 2013). Although there appear to be no cases expressly addressing the issue, it appears likely that directors could face liability under Maryland law if their failure to conduct oversight amounted to gross negligence, especially in circumstances where there are red flags.

15 *See* Zucco Partners, LLC, et al. v. Digimarc Corp., et al., 552 F.3d 981 (9th Cir. 2009); *In re* Countrywide Financial Corp. Derivative Litigation, 554 F.Supp.2d 1044 (C.D.Cal. 2008); *In re* Silicon Graphics Inc. Sec. Litig., 183 F.3d 970, 974 (9th Cir.1999).

Note that Section 17(h) of the 1940 Act sets forth the minimum standard for exculpatory clauses in trust documents by stating that such clauses may not protect a director if he or she demonstrates "willful misfeasance, bad faith, gross negligence or reckless disregard of the duties involved in the conduct of his [or her] office." Accordingly, it seems unlikely that a fund could craft a charter document that would exculpate the directors from responsibility for conduct that was found to violate the standards of *Stone v. Ritter*.

16 *See* Northstar Fin. Advisors, Inc. v. Schwab Invs., *615 F.3d 1106, 1108 (9th Cir. 2010).*

17 As readers are no doubt aware, Target Corp. experienced a cybersecurity breach in the fall of 2013 that resulted in the theft of an estimated 110 million customer records. The cost of the Target breach has been estimated publicly at $148 million. There is a related shareholder derivative action pending against several Target Corp. officers and directors, and the claims against the directors appear intended to align with the *Caremark* standard. Specifically, the plaintiffs alleged that each director knowingly and/or in conscious disregard of his/her duties: (i) failed to implement a system of internal controls to protect customers' personal and financial information; (ii) failed to oversee the company's internal controls system, resulting in inadequate internal controls that failed to protect customers' personal and financial information; and (iii) caused and/or permitted the company to conceal the full scope of the data breach.

18 *In re* Citigroup Inc. Shareholder Derivative Litigation, 964 A.2d 106 (Del. Ch. 2009); *In Re* The Goldman Sachs Group, Inc. Shareholder Litigation, 2011 WL 4826104 (Del. Ch., 2011).

19 The guidance discusses potential cybersecurity disclosure in the following areas applicable to a public company: risk factors, management's discussion and analysis of financial condition, description of the business, legal proceedings, and financial statement disclosures. "CF Disclosure Guidance: Topic No. 2 - Cybersecurity," Division of Corporation Finance (Oct. 13, 2011).

20 The recent decision by a federal district court in Minnesota holding that Target Corp. could be liable to the banks for their expenses in responding to the massive loss of credit card data in Target's 2013 cybersecurity breach shows the potential scope of liability in today's tightly interconnected, mass-market economy. *In re* Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (PAM/JJK) (D. Minn. Dec. 2, 2014).

21 Recent news articles have suggested that some hedge funds have suffered such attacks over the last few years. *See, e.g.,* Nicole Perlroth, "Cybercriminals Zero In on a Lucrative New Target: Hedge Funds," *NY Times* (June 19, 2014). The article discusses that the use of online trading systems by hedge funds makes them vulnerable to hackers who will gain access to the trading information to front-run the fund.

22 NIST released its "Framework for Improving Critical Infrastructure Cybersecurity" on February 12, 2014. The NIST Framework was developed in response to a mandate by Executive Order 13636: *Improving Critical Infrastructure Cybersecurity* that was issued by President Obama in February 2013. The purpose of the NIST Framework is to provide many US industries, including the financial industry, a framework they can use to create, guide, assess or improve

Copyright © 2015 by CCH Incorporated. All Rights Reserved.

comprehensive cybersecurity programs. Similarly, the ISO 27000-series provides recommendations relating to information security management, risks and controls. Commissioner Aguilar, speaking at the "Cyber Risks and the Boardroom" Conference on June 10, 2014, also directed his audience to the NIST framework.

[23] The OCIE sample request list asks about reliance on industry standards, such as those issued by the Commerce Department's NIST or ISO.

Copyright © 2015 CCH Incorporated. All Rights Reserved
Reprinted from *The Investment Lawyer*, February 2015, Volume 22, Number 2, pages 23–36,
with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.wklawbusiness.com

Wolters Kluwer

Copyright © 2015 by CCH Incorporated. All Rights Reserved.