Deloitte.

MFDF

Mutual Fund Directors Forum

Cybersecurity and the evolving threat landscape:

The role of the mutual fund director

April 2022

Table of contents

Introduction/overview 1

Why asset management is an attractive target 1

The board's role in oversight of cybersecurity 2

How does the adviser build a sustainable cybersecurity program? 5

Emerging areas in cybersecurity 10

Synopsis/wrap-up 12

Introduction/overview

Mutual fund directors must navigate an environment where cybercrimes are rising in both number and sophistication. Additionally, a changing regulatory environment compounds the challenges of overseeing cybersecurity. Against this backdrop, fund companies must strive to protect the business against financial, brand, and regulatory impacts of cyberattacks.

Cyberthreats can affect funds, advisers, and shareholders in very concrete ways, including:

- Financial: The **average cost** to an organization for a single cyber incident now **exceeds $1 million**.[1] This includes financial impact from loss of revenue, loss of intellectual property, fines, etc.
- Brand: **65%** of customers affected by a data breach **lost trust in the offending organization**, while **33%** of the people **discontinued their relationship with the organization**. [2]
- Regulatory: Enforcement actions by regulators are increasing, especially related to the mismanagement of personal information. For example, fines can include up to 4% of the annual revenue for non-compliance under the General Data Protection Regulation (GDPR)[3].

Therefore, implementing an effective cybersecurity oversight and governance program is critical to managing cyber risk and the resulting threat landscape.

Increasing threats to mutual funds

As mutual funds increasingly rely on technology to function, cyberthreats have skyrocketed. For example, distribution channels utilizing digital apps are potentially subjected to a greater number of distributed denial of service (DDoS) attacks and client data theft. Ransomware and data theft risks—for both client data and intellectual property—are prevalent across organizations. The threats surface across:

- Front-office operations (including investment strategies, propriety trading algorithms, robo-advisers, and portfolio management);
- Middle-office operations (including compliance reporting, payments and settlements, and risk models); and
- Back-office operations (including fund accounting, reporting, HR, finance, marketing).

Fraud is another materialized cyber risk, perpetrated not only by external actors but also malicious insiders. For instance, settlement and finance systems can be exploited by inappropriate or unmonitored access, as well as data transmission protocols used in the financial sector including SWIFT and FIX systems.

The increasing use of robotic process automation (RPA), artificial intelligence (AI) and machine learning (ML)—without proper controls in place—can further expose firms' cyber vulnerabilities and gaps. Additionally, outsourcing to third parties, cloud service providers as part of digital transformation, and a remote workforce due to the COVID-19 pandemic contribute to an expanded attack surface for malicious actors.

Why asset management is an attractive target

The structure of mutual funds adds complexity to cybersecurity oversight. Often, key functions and operations of funds are performed by third-party service providers, which include the fund's investment adviser (adviser) and any sub-advisers, custodians, distributors, administrators, transfer agents, accountants, and recordkeepers. Each of these service providers may hold critical data that is attractive to cybercriminals and face the risk of cyberattacks with the potential to cause immense financial, brand, reputational, regulatory, and other damage to the adviser, the funds, and their shareholders.

Funds and advisers should continuously reevaluate their cyber risk exposure and establish capabilities to identify, detect, respond to, and recover business processes and infrastructure from cyber events (i.e., establish a formalized cybersecurity program and practice rigor and discipline as cyber risks expand).

The board's role in oversight of cybersecurity

Fund directors are not responsible for designing or overseeing a cybersecurity program. Rather, it is the board's role to oversee management and the adviser's efforts in this area. The board, nonetheless, should remain vigilant and ask key questions about the cybersecurity program.

Fund directors (directors or boards) may find it helpful to view cybersecurity through a risk oversight lens. Directors are responsible for understanding and overseeing how the fund's officers and the fund's adviser manage risk, including in the cybersecurity program, overall risk management, and oversight of the fund's service providers. The tenets of a general risk oversight framework can provide directions to boards as they consider their cybersecurity oversight.

The role of fund directors—including with respect to risk oversight—is grounded in state laws under which a director is a fiduciary to the fund. As a fiduciary, a director owes two basic duties to the fund, the "duty of care" and the "duty of loyalty":

- The duty of care generally requires directors to act with reasonable care and skill in light of their actual knowledge and any knowledge they should have obtained in functioning as a director. Under state law, directors generally are permitted to reasonably rely on experts, including members of management, the fund's adviser, counsel, accountants, and others.
- The duty of loyalty generally means that directors owe a duty to protect the best interests of the fund and not to pursue their own interests, or those of a third party, over the interests of the fund. The duty of loyalty also encompasses the duty to act in good faith.

In assessing claims against directors, courts typically apply the "business judgment rule." The business judgment rule generally insulates a director from liability for a business decision made in good faith if: (i) the director is not interested in the subject of the business decision (i.e., does not have a personal conflict of interest); (ii) is sufficiently informed to make the business decision; and (iii) rationally believes that the business decision is in the best interests of the company.

The Delaware Court of Chancery's *Caremark* decision is widely cited as a baseline for understanding the business judgment rule. [4] The decision emphasizes that directors can show they meet the standards of the rule by establishing—and then periodically monitoring—a reporting or information flow mechanism that responds to either general or particular oversight topics. Following that framework, cases asserting liability for directors generally either claim the board did not receive sufficient information to oversee a risk or consciously ignored "red flags" reported to the board.

Importantly, this framework was specifically applied in litigation that followed a significant 2018 cyber breach involving a hospitality company. The court noted that while "[t]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place," those risks **"do not … lower the high threshold that a plaintiff must meet to plead a Caremark claim"** [5] (emphasis added). In finding the board had acted in accord with the business judgment rule, the court noted regular board reporting, including a discussion of cybersecurity risk in an annual risk inventory; commented that the board knew that both outside consultants and various internal resources were devoted to managing cybersecurity risk; and reviewed information before the board showing internal controls and response plans specifically designed for cyber incidents.

Regulatory guidance

Regulators are increasing their scrutiny of how fund companies protect their organizations and their clients from cyberattacks. The Securities and Exchange Commission (SEC or Commission) and state financial regulators have displayed a high interest in cybersecurity issues over the past decade, and recently the US government has issued executive orders and national security directives in the face of increasingly severe attacks. (While this paper focuses on the expectations of the SEC, as the primary regulator for mutual funds, it is possible that for a particular firm there will be relevant non-US regulatory guidance to consider as well.)

Sources of guidance on SEC and SEC staff expectations for oversight of cybersecurity by funds and advisers include:

- A Division of Investment Management (IM) guidance update from 2015 that provides helpful background for boards as they consider fund cybersecurity; [6]
- Multiple Division of Examinations risk alerts and examination observations related to cybersecurity issues; [7]
- Division of Corporation Finance guidance, primarily related to disclosures and insider trading; [8] and
- Proposed (but not yet adopted) cybersecurity risk management rules for funds and advisers, which we summarize below.[9]

The SEC's proposed cybersecurity risk management rule (Rule 38a-2)

In February 2022, the SEC proposed detailed cybersecurity risk management rules for both advisers (proposed Rule 206(4)-9 under the Investment Advisers Act) and funds (proposed Rule 38a-2 under the Investment Company Act).[10] The centerpiece of proposed Rule 38a-2 is that funds must have a written risk management program devoted to cybersecurity.

Of course, most fund firms already have cybersecurity policies and procedures. These policies and procedures can reflect existing SEC staff guidance, state law requirements (a number of states already require what are called "written information security plans," sometimes referred to as WISPs), and SEC information protection and privacy rules under Regulation S-P or Regulation S-ID. Firms also often consider cybersecurity preparedness to be an element of their overall compliance program under Rule 38a-1 (the compliance program rule). Fund firms will need to maintain these policies and procedures whether or not the SEC adopts cybersecurity risk management rules.

Cybersecurity preparedness requirements likely to be mandated by the proposed rule include:

1. Adoption of policies and procedures tailored to a fund's cybersecurity risk profile and appointment of one or more cybersecurity risk administrators to implement those policies and procedures.
2. Risk assessments, including assessment of risks associated with certain service providers, oversight of such providers, and appropriate written contracts with such providers.
3. Controls designed to minimize user-related risks and prevent the unauthorized access to fund information systems and fund information on those systems.
4. Measures to monitor fund information systems and protect fund information from unauthorized access or use, including through detection, mitigation, and remediation of cybersecurity threats and vulnerabilities.
5. Cybersecurity incident response and recover plans reasonably designed to ensure: (A) continued operations of the fund; (B) protection of fund information systems and fund information on those systems; (C) external and internal communication; (D) reporting of a significant fund cybersecurity incident by the fund's adviser under a proposed confidential SEC reporting mechanism, and (E) written documentation of an incident.
6. At least annual reassessment of the program.

The fund board would be required to initially approve the program and receive an (at least) annual written report. The role of the board—and the general framework for cybersecurity preparedness—envisioned by the proposed rule is consistent with the oversight structures and approaches described by this paper.

Governance structure and the role of the board

It is well established that senior-level engagement is critical for an effective cybersecurity program. Senior management should devote sufficient attention to setting the cybersecurity strategy. In addition, the board should devote sufficient attention to its oversight of the strategy. The Division of Examinations reports emphasize these points. [11]

If adopted, proposed Rule 38a-2 specifically would require board oversight. Following initial approval of a fund's cybersecurity policies and procedures, fund directors over time would review reports on cyber incidents and material changes to policies and procedures. Echoing language used in other SEC releases, the SEC adds that "board oversight should not be a passive activity." [12]

Periodic risk assessment

Given the evolving nature of cybersecurity threats, the SEC staff recognizes that assessment of cybersecurity threats should be dynamic as well. The SEC staff has recommended that advisers and funds understand the cybersecurity threats and vulnerabilities relevant to their businesses. [13] Under Rule 38a-2, this would be structured around an inventory of identified information systems, to be categorized and prioritized based on risk assessment and with an understanding of the roles of different service providers in maintaining and protecting information for the benefit of the funds. The rule would require funds to document these risk assessments in writing.

Assessing potential threats could include understanding: [14]

- The types of information that the fund (directly or through service providers) possesses;
- The technology systems used to collect that information;
- Internal and external threats to information and technology;
- The risks to the fund and service providers should systems become compromised; and
- Controls and processes in place to mitigate cybersecurity risks.

As this list suggests, fund directors would use a common-sense approach to threat assessment, considering each threat from the perspective of the business. For example, if a particular information or technology system may become compromised, business-focused questions could ask which of the firm's business functions would be affected, to what degree and for how long; and then, what are the sources of threats for that system; what are the up-front mitigants; and how would the business manage an actual incident. [15]

Developing a cybersecurity strategy

The IM staff recommended that funds look to the information gathered during the assessment process to design a program that is "designed to prevent, detect, and respond to cybersecurity threats." [16] According to those staff recommendations, the strategy could include:

- Protecting access to data; [17]
- Data loss prevention; [18]
- Data backup and retrieval; [19]
- Incident response planning; [20] and
- Regular testing of the cybersecurity strategy. [21]

Proposed Rule 38a-2 covers similar ground and would require that a fund's cybersecurity risk management program include, in addition to risk assessment as discussed above:

- User security and access standards, including multi-factor authentication (MFA), procedures for passwords, restricting access to employees on a "need to know" basis, and securing remote access technologies;
- Periodic assessments of information systems to support measures to prevent unauthorized access or use of data;
- Cybersecurity threat and vulnerability management; and
- A cybersecurity incident response plan (IRP) intended to improve operational resilience during a significant cyber event and to provide for specific governmental and client reporting.

Effective implementation of the strategy

The IM staff recommended that implementation of the cybersecurity strategy include: [22]

- Written policies and procedures;
- Training officers and employees regarding threats and measures to prevent, detect, and respond to such threats; and
- Client education to reduce risk of exposure of client accounts.

In addition to staff guidance outlined above, enforcement actions can provide useful information about the Commission's views on cybersecurity. The SEC's Division of Enforcement has established a cyber unit to focus on, in part, cybersecurity controls at regulated entities. In three recent enforcement actions, the SEC sanctioned eight SEC-registered firms for alleged lax cyber controls and cybersecurity failures involving cloud-based email systems. [23]

How does the adviser build a sustainable cybersecurity program?

Advisers and other key service providers can choose from among various frameworks to develop their cybersecurity programs. While a deep understanding of these programs is beyond the scope of the role of directors, a broad appreciation can help boards organize their oversight and identify key questions of interest. (This paper refers frequently to "the adviser" and "the adviser's cybersecurity program." That choice of language reflects the central role of the adviser for most fund firms but is not intended to suggest that funds will not have their own cybersecurity programs or to diminish the role that a fund's officer or providers beyond the adviser may have at a particular firm.)

The five-step framework suggested by the Association of International Certified Professional Accountants, laid out below, can help fund complexes prevent, detect, and mitigate cybersecurity incidents. The steps also can provide a helpful outline for board oversight and understanding. The steps include:

- Identifying and communicating what needs to be protected;
- Assessing and classifying roles;
- Developing and prioritizing processes;
- Responding and enforcing; and
- Continuously learning and evolving.

The discussion below is intended to provide boards with possible approaches for board oversight and understanding, not to endorse any particular framework. In addition to the Association of International Certified Professional Accountants framework, there are many others that are used by advisers and other service providers to structure their cybersecurity programs. In addition, the questions suggested below may not be appropriate for all fund boards; cybersecurity oversight varies significantly based on the size and complexity of the fund complex, among other factors.

Identify and communicate what needs to be protected

A cybersecurity program should begin with management or the adviser mapping out key assets (e.g., information, data, personal information, IT systems) and assessing who may want to target them—both the how and why and the relative likelihood of occurrence.

In assessing whether the adviser has appropriately considered the cybersecurity risks to the fund complex, directors may wish to ask questions such as:

- What are the greatest cybersecurity threats our fund complex faces?
- What are the "crown jewels" that we must protect, including data and other assets?
- Does the inventory consider material business information, personal information, and all systems required for fund operations?
- Does the adviser have an appreciation for the potential avenues of a cyberattack?

Given the nature of the fund industry, however, the adviser is not the only entity that requires board focus. In addition to the fund's adviser, a web of third parties provides critical services to funds. These service providers may have access to critical information that may be targeted in cybersecurity incidents. In order to identify and communicate what needs to be protected with respect to third-party service providers, the adviser should have a thorough understanding of all service providers that the funds employ, what information those service providers can access as well as how they interact with the adviser's own systems and data. Lastly, it is critical to understand if the third-party service providers in turn outsource or offshore any activities that may present "fourth-party risk" and beyond. Directors may wish to ask whether the fund (generally acting through the adviser) has:

- A robust inventory of third-party service providers;
- A robust inventory of the critical data that is gathered, used, and/or maintained by the third party;
- A process in place to monitor how the third-party accesses the fund's or adviser's own systems and data;
- An understanding of outsourcing or offshoring to additional parties; and
- A process to rank the cybersecurity risks posed by the fund's third-party service providers.

Assess and classify roles

Having the right personnel in place and establishing clear roles and responsibilities are critical in establishing an effective cybersecurity program. A cybersecurity program is only as effective as the personnel responsible for it. The adviser may choose to use its own personnel or to outsource many cybersecurity activities to an appropriate third party. In addition, the adviser needs to assign responsibility for cybersecurity in a way that aligns with the size, structure, and complexity of the fund complex.

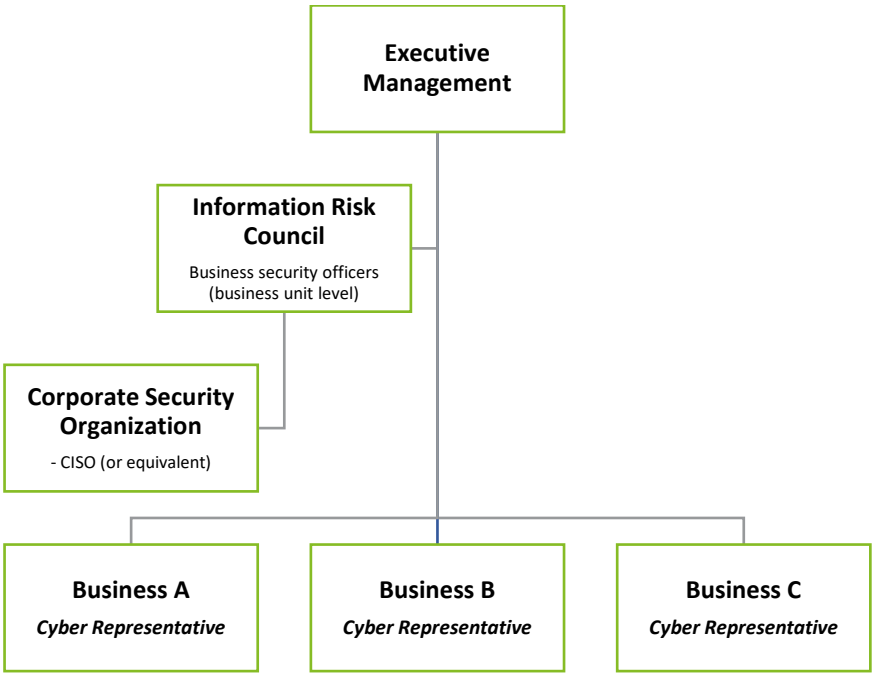
The adviser determines how to staff its cybersecurity program—whether attracting individuals to build an in-house program or by hiring a third party to handle cybersecurity. Identifying and hiring cybersecurity personnel can be a significant challenge. With too many facets to consider, too many vulnerabilities, and too few IT professionals to manage every threat, many organizations are having to outsource their cyber operations. According to Deloitte's Future of Cyber Survey 2019, 85% of participants indicated some level of reliance on vendors and managed service providers to handle cybersecurity operations—and two-thirds of those outsourcing between 21% and 50% of cyber operations. [24]

With respect to staffing of the cybersecurity program, directors may wish to ask:

- Does the adviser use in-house personnel for cybersecurity? If so,
  - How does the adviser evaluate whether these personnel are appropriately trained?
  - Has retention been an issue with cybersecurity personnel within the organization?
  - Does the adviser have all the cyber resources it needs to execute its cyber risk program?
- If the adviser uses a third-party service provider for cybersecurity, directors may wish to ask:
  - Is the adviser satisfied with the level of service provided?
  - What type of initial due diligence did the adviser conduct?
  - How does the adviser conduct ongoing due diligence?

Once appropriate personnel are in place, whether in-house or by using a service provider, the firm must then determine how to structure cybersecurity oversight. As in many other areas of risk management, tone at the top is critical. Regardless of the level of third-party reliance, executive management of the firm should play a critical role in the process.

Some organizations have recognized the benefits of embedding cybersecurity professionals throughout the business. Integrating cyber liaisons across an adviser can help firms achieve alignment on priorities—and prevents siloed agendas, or worse, having to remediate incidents that could have been prevented—and is becoming an emerging consideration for advisers. Today, the trend at many financial services organizations is to have business security officers embedded in the business units. Larger advisers and other mutual fund service providers may consider and adopt a similar structure in their organizations. The illustration below outlines what this might entail. This is consistent with the emphasis on the first line to manage enterprise risks.



In assessing how well embedded cybersecurity is in all aspects of the adviser's (or other key service provider's) business, directors may wish to ask:

- What is the reporting chain for cyber professionals at the adviser?
- Are there cyber professionals in each major business unit? If not, how do the cyber professionals monitor each business unit?
- How do the business teams work with cyber professionals when developing new products or services?
- Do business leaders know who to contact either in the event of a cyber incident (or suspected incident) or when planning a new project?

Develop and prioritize processes

Key to developing an effective cybersecurity program is defining the firm's cybersecurity risk tolerance (sometimes also referred to as risk appetite). The process can include defining acceptable levels around downtime for digital channels; assessing the trade-off in the customer experience between good security; and evaluating ease of use for clients, to name just a few. After the thorough assessment, the risks should be integrated into the firm's enterprise risk management framework. In order to better appreciate cybersecurity risk tolerance and how that impacts broader risk management, directors may wish to ask:

- How does the adviser think about its risk tolerance with respect to cybersecurity?
- Are key cybersecurity risks measured against that risk tolerance?
- How do cybersecurity risk efforts inform broader enterprise risk considerations at the adviser?

The adviser should develop processes and procedures designed to manage the organization's cybersecurity risks in accordance with its risk tolerance. Policies and procedures designed to manage cybersecurity risks will vary considerably across funds based on the size and complexity of the fund complex and other factors unique to each adviser. In overseeing the adviser's cyber risk management process, directors may consider the following:

- How is the adviser managing risk and ensuring that risk is reduced to an acceptable level?
- What is management's approach for investing and allocating resources to monitor cyber risk, guard against it, and expedite response and recovery?
- How is the return on security spending and program effectiveness in managing cyber risks evaluated?

As discussed above, advisers typically rely on other third-party service providers to perform the day-to-day functions necessary to run the funds in the complex. Those service providers can pose considerable cybersecurity risks to the fund and the adviser; therefore, managing those risks is critical to establishing an effective cybersecurity program. Given their importance, directors should appreciate how the organization manages the risk posed by third parties and may wish to ask:

- Has the adviser established integrated and automated processes to improve the efficiency and integration of the third-party life cycle including onboarding, due diligence, contract, and ongoing monitoring of existing or new third parties?
- Is accountability of third-party oversight embedded within the business, and are there clear roles and responsibilities for ongoing monitoring?
- Has the adviser improved transparency into risk management capabilities and controls of fourth and fifth parties?
- Is the adviser promoting proactive and intelligence-driven cyberthreat monitoring of third parties, including targeted data protection reviews, and obtaining increased visibility into the hosting organization's data of third-party environments?

Respond and enforce

An effective cybersecurity program requires that the firm be prepared to develop and enforce policies and procedures to govern the process and respond to inevitable cybersecurity incidents. A cybersecurity program cannot be expected to prevent every cybersecurity intrusion; however, the program should be reasonably designed to detect intrusions and mitigate the damage to the extent practicable.

Because cybersecurity incidents are inevitable, it is critical that the adviser have appropriate procedures in place in the event of a crisis. For example, the plan needs to consider how the adviser will respond to the crisis, including who is involved in the response and what the response will be; how it will ensure that the fund has access to critical services; and how critical data can be recovered in the event of a loss. As directors consider preparedness for a cybersecurity incident, they may wish to ask:

- Is the cybersecurity program adequately staffed and funded?
- How are incidents handled and reported?
- How is the cybersecurity program tested? Does the testing take place regularly?
- What are the protocols for reacting to a cybersecurity incident? Are those protocols well defined and understood across the organization?
- Does the firm conduct simulation exercises to improve readiness for a cybersecurity intrusion?
- With respect to third-party service providers, has the firm conducted a deep dive of contract terms to determine the respective responsibility for cybersecurity incidents? In the event that a contract is silent, have other mechanisms been agreed to assign responsibilities in the event of a cybersecurity attack?
- How do business continuity and disaster recovery plans consider cybersecurity issues?

A key component of a functioning cybersecurity program is well-defined communication protocols. As the board and the adviser consider a proper communication protocol, considerations include the reporting schedule, the key personnel who report to the board, where oversight of cybersecurity resides on the board, and the content of such reporting. Questions for boards to consider regarding communication include:

- What is the reporting schedule? The reporting schedule determined by the board and adviser should be sufficient to provide appropriate oversight. Depending on the size and complexity of the funds and their adviser, the board could determine whether the reports are every meeting or some other appropriate schedule. In addition to regular reporting, the board and adviser should determine when the board should be notified of critical cybersecurity issues. The board and adviser can agree on a threshold and time limit in light of the facts and circumstances of the event.
- Who reports to the board? The board and management also should discuss who should give that report to the board, whether it is the chief information security officer or another member of the cyber team. The chief compliance officer may be helpful in guiding the board regarding the appropriate personnel based on the particular cybersecurity issue to be discussed.
- Where does cybersecurity responsibility reside on the board? Boards may wish to designate a committee to have primary oversight responsibility or determine that the responsibility should remain with the full board. If a board chooses to have a committee oversee cybersecurity, the committee should consider how to best share critical information with the full board to facilitate effective oversight. In addition, the board may consider designating a point person to be notified of critical cyber incidents between meetings.
- What type of reporting does the board receive? In addition to determining where the oversight of cybersecurity should reside, determining the appropriate reporting also is critical. Given the technical nature of cybersecurity issues, boards must work with management to make sure the reporting is understandable to the board and provides the information critical to providing effective oversight.

Continuously learn and evolve

The fund complex continues to change and evolve and may add or change third-party service providers to better serve the funds. In addition, the nature of the risk to the funds may change substantially based on how the fund uses technology. Finally, the nature of cybersecurity threats is not static—bad actors continuously change the way they conduct their cyber intrusions. As a result, cybersecurity programs must be reevaluated and updated regularly to reflect current realities. When boards consider the adviser's actions in this area, they may wish to ask:

- How often does the adviser review its cybersecurity policies and procedures?
- Do advisory personnel and the board receive regular education on emerging cybersecurity threats? For example, advisers may receive a "root cause" analysis of cyber incidents or a "why not here" analysis of industry cyber incidents.
- Are cybersecurity incidents shared across the organization to allow the organization to learn from past events?
- Does the adviser participate in information-sharing opportunities to stay abreast of emerging threats?

Cybersecurity insurance

Given the risk of substantial loss due to a cybersecurity incident, boards may wish to discuss with management, counsel, and their insurance broker the availability of insurance [25] to cover the losses and expenses incurred as a result of a cybersecurity incident, and whether such insurance is appropriate for the fund complex.

As in other aspects of cybersecurity, cybersecurity insurance has evolved as insurers gain additional expertise with this area—and as cybersecurity issues continue to evolve. As directors begin to think about this area, they may wish to consider:

- Who holds the policy? It may be more common for the policies to be held by the adviser or other service provider rather than the funds directly.
- Who are the insureds under the policy?
- What does the policy cover, and are there important exclusions from coverage to consider?
- Is cybersecurity treated in any particular way, either explicitly or implicitly, under a fund's or adviser's base insurance policies?
- How will different kinds of policies, providing for different types of coverage at different places in the organization and potentially with different insurers, interact with each other?

Emerging areas in cybersecurity

With digital transformation comes the cyber evolution

Most advisers and mutual fund organizations are undergoing dramatic and expansive business and digital transformations driven both by market needs and the pandemic. Boards should be aware of the potential cyber impact of these efforts and how the adviser and key service providers are managing the resulting risks. The following section highlights the cyber impact of some of these key transformation efforts.

Does the ease of automation create greater risk?

Two key business transformations within fund complexes are the increasing use of RPA and AI/ML. RPA and AI/ML enable automation, augment human decision-making, and deliver rapid business value. Asset management and mutual fund organizations are increasingly deploying RPA and AI/ML technologies to gain process efficiencies from automation and analytics. RPA and AI/ML are also being leveraged across advisers to help identify common traits or unexpected events within vast data sets, stitch together nuanced data insights, and interpret data rapidly and at scale. These technologies also help address the rising training and operations costs for human resources and lack of skilled talent.

However, this shift toward increased implementation of RPA and AI/ML technologies increases the attack vectors that adversaries can use to target organizations and poses heightened security challenges:

- RPA technology introduces a new attack surface to gain unauthorized access. RPA software typically requires privileged access (or access above and beyond a standard user) to perform tasks. Often, developers will "hard code" the access into the script or it may include a step to retrieve the credentials from an unsecure location. Hard-coded, shareable credentials can be stolen by a malicious insider or a cyberattacker and allow them to move across the network, giving them access to encrypted data systems.
- Similar cyber risks exist for AI/ML enhancements. In addition, the amount of data needed to train the machine elevates the cyber risk. Massive amounts of data are needed to train the predictive model; test data is needed to see how well the model works; and live, transactional data is being consumed when the model is put to work.
- IT organizations may overlook the data protection needs of the training and testing data, thus allowing greater access to the data.

Advisers should consider how their cybersecurity programs need to evolve to address the unique risks of these technologies. As a result, directors may find it useful to ask how the adviser has addressed the following potential issues:

- Does the adviser have the capability to identify, detect, and respond to RPA and AI/ML-based emerging threats, including reinforcing secure development practices?
- How is the adviser going to work to maintain the confidentiality and integrity of information stored/processed using RPA and AI/ML, including the algorithms and models?
- Have the IT experts worked with those in the fund complex who own the business continuity planning (BCP) or disaster recovery planning to ensure continuous availability of services?

How secure is the cloud?

The previous decade saw the emergence of cloud and cloud-enabled technologies resulting in a shift in the way organizations view their businesses. Cloud adoption has enabled advisers to improve agility, enhance automation, and go to market faster. Digital transformation and cloud adoption raise several potential cyber risk areas, including:

- Dispersed cloud governance that may lead to fragmentation of cloud security capabilities across the enterprise; tension between business-driven cloud security objectives and centralized governance; and lack of controls responsibility and integration with the existing enterprise;
- Managing data risk in the cloud including challenges in understanding and managing data risks and privacy concerns for cloud; data stored in misconfigured cloud services that could expose sensitive information and implications of relevant regulations;
- Compromised security when a rush to move to cloud takes precedent over security, allowing vulnerabilities to creep into the design and code;
- Lack of Identity and Access Management (IAM) for cloud assets as well as gaps in managing new users and third-party access requirements; and
- Limited planning for redundancy and preparedness for cloud service provider failure.

Some considerations for the directors to ask related to cloud security include:

- Has the adviser identified the baseline security requirements for cloud environments that are in line with the organization's risk tolerance?
- Has the adviser established controls and roles and responsibilities specific to the cloud to address governance and technology gaps that will support risk reduction efforts?

- How does the adviser manage user identities across the cloud platform and related applications?
- Has the adviser established rapid response capabilities for security incidents or failures through automation?

With virtual work comes virtual risk

The COVID-19 pandemic has resulted in an abrupt shift in how businesses operate in both the short and long term. Many advisers are now realizing the financial or operational benefits of a virtual operation. Advisers should ensure that their employees have the necessary equipment, working practices, access rights, and technology to work in a virtual office environment, especially with the need to minimize contact and business and community disruptions. Insider threat programs may need to be reevaluated as many organizations will look at previous patterns of work behavior to establish baselines for identifying anomalous activity within their networks or applications. Other key cybersecurity risks are also present as the attack surface continues to expand with a virtual workforce include:

- Personnel may use virtual collaboration and data-sharing tools that have not been fully vetted by the security organization or have unidentified/non-remediated vulnerabilities.
- Personnel may inappropriately share/store sensitive information via virtual collaboration and data-sharing tools.
- Remote employees may be tricked into providing sensitive information through phishing emails or social engineering.
- Remote access infrastructure may lack capacity for increased usage.
- Inappropriate use of personal devices that may lack appropriate security measures and monitoring mechanisms—which can result in employees accidentally exposing sensitive data—purposely taking fund and shareholder data, as well as increased risk of adversaries trying to compromise these devices.

Key questions board members may consider include:

- Does the adviser's overall approach to cybersecurity work in light of the transition to work from home?
- Has the adviser enhanced the organization's IT infrastructure to manage the increased scale of remote access and volume of network traffic?
- Has the adviser enhanced the organization's remote access controls to provide appropriate security (e.g., MFA) for continuous or increased volume of remote access to internal networks?
- Has the adviser bolstered its existing insider threat monitoring programs and targeted monitoring of insider and third-party activity?
- Is the adviser raising security awareness and increasing threat detection and response to promote proactive identification of malicious activity?
- Does the adviser have policies, controls, and monitoring capabilities over the use of remote firm-issued hardware and employee personal electronic devices?
- Has the adviser adapted employee training and policies based on lessons learned from virtual operations?

Synopsis/wrap-up

The starting point for an effective cybersecurity program begins with proper governance for cyber risk. Executive leadership should support the board's need to understand the design and effectiveness of cybersecurity controls. The board's understanding begins with an open dialogue with management regarding the key areas of cyber risk in the fund complex. From there, management should be clear about how it has built its cybersecurity program, including that personnel responsible for cyber have the appropriate skills, resources, and approach to minimize the likelihood of a cyber incident—and the ability to detect and mitigate any potential damages when one does occur.

Board members should continue to educate themselves on how to include appropriate oversight of cybersecurity as part of their overall risk oversight efforts. While cybersecurity is rapidly evolving and sometimes technically complex, directors are tasked with:

- Understanding the broad nature of the key threats;
- Asking management how risks are being mitigated and managed;
- Being informed on how cyber risk and data security incidents are identified, and what response protocols are in place; and
- Understanding key cyber risks that may impact the fund complex and effective oversight of the cybersecurity program.

Like other oversight roles, directors are empowered with exercising their business judgment over cybersecurity-related issues. In order to do so, boards should have the right information and ask the right questions based on risks to the organization. For boards of directors to be effective there must be a shared understanding between senior management, technology executives, and directors of how these complex technical issues impact business-critical risks across the value chains of advisers, fund complexes, and third-party service providers; how they are detected; and the governance around escalation, communication, and reporting protocols.

Mutual Fund Directors Forum Cybersecurity Oversight Working Group

Sameer Airyil, Senior Manager, Deloitte & Touche LLP

Colleen Brown, Partner, Sidley Austin LLP

Krissy Davis, Vice Chair, US Investment Management Leader, Deloitte & Touche LLP

Nathan Greene, Partner, Sidley Austin LLP

Thomas Hayden, Board Chair, Oakmark Funds

Paul Kraft, Partner, Investment Management Brand and Eminence Leader, Deloitte & Touche LLP

Peg McLaughlin, Director, Manning and Napier Funds

Lloyd Wennlund, Board Chair, Datum One Series Trust and Director, Calamos Funds

Christopher Wilson, Board Chair, Invesco Funds

Endnotes

[1] US Executive Office of the President, "Cost of malicious cyber activity to the US economy," Council of Economic Advisors, February 2018.
[2] The impact of data breaches on reputation & share value: A study of US marketers, IT practitioners and consumers," Ponemon Institute LLC, May 2017.
[3] https://gdpr-info.eu/issues/fines-penalties/
[4] *In re Caremark Int'l Deriv. Litig.*, 698 A.2d 959 (Del.Ch. 1996)
[5] *Firemen's Retirement System of St. Louis v. Sorenson, et al.*, C.A. No. 2019-0965-LWW.
[6] US Securities and Exchange Commission (SEC*), IM Guidance Update*, No. 2015-02, April 2015 ("IM Cybersecurity Guidance").
[7] SEC, *Cybersecurity and resiliency observations*, Office of Compliance Inspections and Examinations, January 27, 2020 ("Cybersecurity Observations").
[8] SEC, *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, Division of Corporation Finance, October 13, 2011.
[9] *See* Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release Nos. 33-11028; 34-94197; IA-5969; IC-3449, February 2022. Available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf. ("38a-2 Proposing Release")
[10] Securities and Exchange Commission (SEC), "SEC proposes cybersecurity risk management rules and amendments for registered investment advisers and funds," press release 2022-20, February 9, 2022.
[11] *See* Cybersecurity Observations.
[12] *See* 38a-2 Proposing Release.
[13] The SEC staff has recommended that advisers and funds understand the cybersecurity threats and vulnerabilities relevant to their businesses.
[14] *See* IM Cybersecurity Guidance.
[15] Ibid.
[16] This focus on cybersecurity oversight from the perspective of correlating risk with specific business functions is discussed in Parenty, T. & Domet, J. Sizing up Your Cyberrisks. *Harvard Business Review* (2019).
[17] *See* IM Cybersecurity Guidance at 2.
[18] *See* IM Cybersecurity guidance. *See also* Cybersecurity Observations.
[19] *See* IM Cybersecurity Guidance.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] SEC, "SEC announces three actions charging deficient cybersecurity procedures," press release 2021-169, August 30, 2021.
[25] *See* IM Cybersecurity Guidance.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.