The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 28, NO. 6 • JUNE 2021

Sleepless over Cybersecurity: Legal Duties and Best Practices for Investment Company Directors

By Kate H. Campbell, Ellen R. Drought, and Margaret L. Johnson

Fund directors have been responsible for oversight of fund cybersecurity programs as part of their risk management and governance functions for many years.[1] In keeping with the importance of this topic, the Securities and Exchange Commission (SEC) has issued regular guidance on cybersecurity practices of funds, investment advisers, and broker-dealers, issuing three alerts related to cybersecurity in 2020 alone. Cybersecurity remains a focus area in the SEC's Division of Examinations *2021 Examination Priorities*, which notes that the Division is "acutely focused on working with firms to identify and address information security risks, including cyber-attack related risks . . . ." The SEC considers governance around cybersecurity to be of paramount importance.[2]

There has been less guidance about the individual cyber responsibilities of fund directors themselves, even as their use of technology continues to evolve. Fund directors have developed various practices regarding email, text messaging and digital board book portals in conducting fund business over the years. While some funds require directors to use company-provided devices and email addresses, other directors use personal tablets, laptops or smartphones, and personal or other business email addresses for fund communications. According to a 2018 study commissioned by Diligent Corporation, 56 percent of board members surveyed use personal email for board-related communications.[3] While some fund boards continue to use physical board books, others have adopted digital board book portals provided by third party service providers such as Nasdaq and Diligent, which offer a secure (but not risk-free) platform for board meeting materials and communications.

As fund board meetings transitioned to a virtual setting in 2020 as a result of the pandemic, the cyber issues faced by directors grew quickly. Directors were required to navigate the novelty of virtual meeting platforms in a work-from-home environment while at the same time engaging in more frequent meetings and communications in response to increased market volatility, the implementation of business continuity plans, financial pressures, shareholder redemptions, and other concerns. At the same time, cyberattacks began to rise as cybercriminals sought to take advantage of potential weaknesses of work-from-home technology.[4]

In light of the rapidly evolving use of technology in recent years and months and the attendant risks, fund directors should consider legal and practical considerations governing their cyber practices when conducting fund business. This article reviews

applicable law, regulatory guidance, and policies and procedures governing the cyber practices of fund directors. The article also provides recommendations as to good cyber "hygiene" and other practices fund directors may consider adopting with respect to their own data management programs as a means of minimizing risk to themselves and the funds they oversee. While there are risks and benefits associated with different cyber practices, fund directors should consider adopting dedicated email addresses for fund business, limit the amount of sensitive data transmitted via email (or text message), and use due care when navigating digital board book portals and virtual meeting platforms. Funds also should consider adopting or enhancing policies surrounding director communications and technology to address recent developments and evolving risks, engage in boardroom discussions around these topics, and provide educational opportunities to fund directors about cybersecurity.

Legal Framework for Board Cybersecurity Practices

Fiduciary Duty

In executing oversight and decisionmaking functions over risk management topics such as cybersecurity (including their own data practices), fund directors owe fiduciary duties to the fund and its shareholders under the laws of the state in which the fund is organized. Fiduciary duty has been developed under case law and is comprised of two main duties: the duty of loyalty and the duty of care.[5] The duty of loyalty requires fund directors to act in good faith and to place the interests of the fund ahead of the director's own self-interest or the interest of another person or organization with which the director is associated. The duty of confidentiality, which is generally understood to fall within the scope of the duty of loyalty, may be implicated by a fund director's personal cybersecurity practices.[6] A director may breach his or her duty of confidentiality by inappropriately disclosing confidential fund information, regardless of whether the disclosure was deliberate or accidental.[7] The duty of loyalty also could apply with respect to a fund director's personal cybersecurity practices in the context of bad faith or a conflict of interest, such as through a director's association with a technology vendor that provides a personal benefit.

The duty of care requires that a fund director perform his or her duties in good faith and in a manner reasonably believed to be in the fund's best interests. The duty of care provides that a fund director should act with the reasonable care and skill that an ordinarily prudent person in a like position would exercise under similar circumstances.[8] A fund director's duty of care may come under review should the director act negligently (or unreasonably) with respect to his or her own personal cybersecurity practices, particularly if the director's lax approach toward cybersecurity results in a breach that causes monetary or reputational harm to the fund or its shareholders. A fund director's duty to understand the cybersecurity risks he or she faces as a director, and how best to mitigate those risks, also implicates the director's fiduciary duty of care to the fund and its shareholders.

Section 36(a) of the Investment Company Act of 1940 (1940 Act) also imposes a fiduciary duty on fund directors and authorizes the SEC to bring an action against a fund director for a breach of fiduciary duty involving "personal misconduct" with respect to a registered fund. Courts have disagreed as to the interpretation of the "personal misconduct" standard, including as to whether Section 36(a) applies only where self-dealing and conflicts of interest are involved, and the SEC has not provided guidance as to the meaning of fiduciary duty under Section 36(a). The SEC has brought very few actions against fund directors alleging breach of fiduciary duty under Section 36(a); and while private litigants continue to attempt to bring a private cause of action under Section 36(a), courts generally have held that Section 36(a) does not authorize private rights of action.[9] Accordingly, the cyber practices of

fund directors are most likely to be evaluated under state law fiduciary duty standards or under the SEC guidance discussed below.

Risk Management and Cybersecurity Laws and Regulations

1940 Act

Managing cybersecurity risk is part of a fund's risk management program. While fund directors are not responsible for day-to-day risk management, they are responsible for overseeing the fund's, adviser's, and other service providers' risk management practices, including cybersecurity.[10] Though risk oversight is part of a board's fiduciary duty under state law, risk oversight is not specifically set forth in SEC rules adopted under the 1940 Act; however, a fund director's risk oversight function is associated with various provisions of the 1940 Act, including Rule 38a-1, which requires a fund's board of directors to approve the fund's compliance policies and procedures and those of certain service providers.

A board's oversight function includes understanding the regulatory, investment, and operational risks of the fund, assessing the effectiveness of risk practices and controls of service providers, and evaluating whether fund policies and procedures are reasonably designed and effective to prevent the violation of applicable federal securities laws.[11] In overseeing cybersecurity risk, fund directors often: (1) review cybersecurity programs and incident response plans of the fund and the fund's investment adviser and transfer agent, among other key service providers; (2) ensure that service provider contracts contain sufficient provisions regarding the implementation of information security programs; and (3) discuss the types of shareholder data and other sensitive information maintained by service providers to the funds.[12] Boards may also consider whether the fund and its service providers have procured cyber-liability insurance to cover the costs of a cyber-attack, as discussed below.

Other State and Federal Laws

There are a growing number of state and federal laws that require funds to maintain appropriate levels of cybersecurity,[13] including the Gramm-Leach-Bliley Act (GLBA) Privacy Rule and Safeguards Rule[14] and in the New York Department of Financial Services (NYDFS) Cybersecurity Regulation.[15]

GLBA Privacy Rule and Safeguards Rule. The GLBA contains a Privacy Rule that requires financial institutions to inform customers about how customers' personal information is collected and to comply with certain limitations on how that information is disclosed.[16] The GLBA Safeguards Rule then requires financial institutions to protect that personal information.[17] To the extent a financial institution experiences a data breach, both violations of nondisclosure requirements under the Privacy Rule and the cybersecurity requirements in the Safeguards Rule may be implicated.

The purpose of the GLBA Safeguards Rule is to set "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[18] Customer information means "any record containing nonpublic personal information . . . about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates."[19] The Safeguards Rule requires that an entity "develop, implement, and maintain a comprehensive information security program" that "contains administrative, technical, and physical safeguards that are appropriate to [the entity's] size and complexity, the nature and scope of [the entity's] activities, and the sensitivity of any customer information at issue."[20] Such policy must be "reasonably designed" to "(1) [i]nsure the security and confidentiality of customer information; (2) [p]rotect against any anticipated threats or hazards to the security or integrity of such information; and (3) [p]rotect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."[21]

To the extent shareholder information is included in fund director communications, whether in meeting minutes, board materials or email communications, the Safeguards Rule certainly would apply to the security and confidentiality of such information. Further, many fund privacy policies adopted under GLBA take a more expansive view of the type of information that is deemed confidential and may cover a broader range of fund-related communications. In addition to avoiding email or other electronic communications to transmit sensitive information, fund directors should take further precautions when handling any communications that include shareholder data, such as only using a password-protected board portal or communicating via telephone or in a board meeting about such topics.

NYDFS Cybersecurity Regulation. In 2017, NYDFS enacted the Cybersecurity Regulation and has since implemented related policies and controls.[22] While many funds may not fall under the purview of the Cybersecurity Regulation, the framework adopted by the state of New York may foreshadow forthcoming cybersecurity requirements on a state or federal level as the calls for more data privacy regulation grow.

Like the GLBA Safeguards Rule, NYDFS's Cybersecurity Regulation requires that a covered entity maintain a cybersecurity program "designed to protect the confidentiality, integrity and availability of the covered entity's information systems."[23] The program must be based on the entity's risk assessment and be designed to:

1. Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;
2. Use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;
3. Detect cybersecurity events;
4. Respond to identified or detected cybersecurity events to mitigate any negative effects;
5. Recover from cybersecurity events and restore normal operations and services; and
6. Fulfill applicable regulatory reporting obligations.[24]

The Cybersecurity Regulation requires that an entity's cybersecurity program be in place and that "all personnel" receive cybersecurity awareness training.[25] While fund directors may not be among the personnel required to receive this training, funds may wish to invite their directors to training related to the fund's cybersecurity policies and procedures to protect nonpublic information, given the nature of the sensitive information that is included in board meeting materials and discussed during board meetings.

SEC Guidance on Cybersecurity

The SEC has increased its focus on cybersecurity in light of the surge in cyberattacks since the COVID-19 pandemic and has issued numerous risk alerts and other publications providing guidance to investment advisers, broker-dealers, and investment companies. [26] While the SEC has not released specific guidance as to how fund directors can mitigate risks associated with their own personal cybersecurity practices, the SEC's cybersecurity guidance provides helpful information to all members of the investment industry, including fund companies and board members.

In cybersecurity guidance issued in 2015 to investment companies and investment advisers, the SEC's Division of Investment Management (Division) noted the "rapidly changing nature of cyber threats," highlighted the importance of cybersecurity and discussed a variety of measures that funds and advisers may wish to adopt when addressing cybersecurity risks. The guidance noted that firms should consider conducting a periodic assessment of (1) "the nature, sensitivity and location of

information that the firm collects" and the technology systems it uses; (2) "internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems"; (3) security controls and processes; (4) the impact of any compromised systems or information; and (5) the "effectiveness of governance structure for the management of cybersecurity risk." Additionally, the guidance suggested firms create a strategy "designed to prevent, detect and respond to cybersecurity threats," such as through the use of authentication and authorization methods, data encryption, the management of user credentials and data and the development of an incident response plan. The Division encouraged firms to implement this strategy through written cybersecurity policies and procedures and training regarding cyber threats and measures to prevent, detect and respond to such threats.[27]

In a January 2020 *Cybersecurity and Resiliency Observations* publication, the SEC's Office of Compliance Inspections and Examinations (now known as the Division of Examinations) (OCIE) discussed industry practices with respect to cybersecurity risk. The report stated, "[r]ecognizing that there is no such thing as a 'one-size fits all' approach, and that all of these practices may not be appropriate for all organizations, we are providing these observations to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency." The publication discussed SEC Staff observations in various areas, including governance and risk management, access rights and controls, data loss prevention, security around mobile devices and applications, vendor management and training and awareness. The SEC Staff observed that the increased use of mobile devices and applications can create additional cybersecurity vulnerabilities and noted several security measures that firms are utilizing to mitigate associated risks.[28] In particular, OCIE cited the establishment of policies and procedures for the use of mobile devices, training of personnel on mobile device policies, access management controls such as multi-factor authentication for authorized users and security measures to prevent printing, copying, pasting or saving information to personally owned computers, smartphones, or tablets.[29] All financial services market participants, including fund companies and their directors, may wish to consider implementing similar policies to prevent the misuse of mobile devices.

In a July 2020 risk alert regarding ransomware attacks, OCIE observed an increase in sophistication of ransomware attacks on investment advisers, broker-dealers, and investment companies.[30] As described in the alert, ransomware "is a type of malware designed to provide an unauthorized actor access to institutions' systems and to deny the institutions use of those systems until a ransom is paid."[31] OCIE noted several measures used by firms to prevent ransomware attacks, including assessing incident response and resiliency policies and procedures, managing user access to computer systems through requiring the use of strong, and periodically changed, passwords, the use of multi-factor authentication and the re-certification of users' access rights on a periodic basis.[32] Firms observed by OCIE also implemented "perimeter security" to monitor, control, and inspect incoming and outgoing network traffic to prevent unauthorized traffic through the use of firewalls, email security capabilities, and intrusion detection systems.[33] Applying this guidance to individuals, it should be noted that personal email accounts may be more susceptible to ransomware attacks as certain filters and spam protections that try to weed out such emails may not be in place as commonly as they are for corporate email accounts.

As part of its response to the COVID-19 pandemic, OCIE issued a risk alert in August 2020 to discuss "new operational, technological, commercial and other challenges" facing investment advisers and broker-dealers.[34] OCIE identified COVID-19 risk areas involving the protection of investor assets and supervision of personnel, and encouraged firms to modify their practices to address various risk points, including communications occurring outside of the

firm's systems in light of personnel working remotely and using personal devices.[35] In addition to suggesting that firms consider whether any compliance policies and procedures used under "normal operating conditions" need to be updated to address the risks of remote operations, OCIE also suggested that firms modify or enhance their security and support for facilities and remote sites and consider operational modifications in order to secure servers and systems, provide support to personnel working remotely and to protect data at remote sites.[36]

In the August 2020 COVID-19 alert, OCIE focused on the protection of sensitive information, noting that the "staff has observed that many Firms require their personnel to use videoconferencing and other electronic means to communicate while working remotely" and that such practices can create vulnerabilities around investors' personal information. Accordingly, OCIE recommended that firms pay particular attention to risks "regarding access to systems, investor data protection and cybersecurity." OCIE encouraged firms to assess their policies and procedures and consider various steps to prevent misuse of investor data, including additional training regarding phishing and other cyber-attacks, communicating the risk of sharing information while using unsecure remote systems, encouraging the encryption of documents and use of password-protected systems, as well as the destruction of paper records used at remote sites. The alert also encouraged firms to consider "[u]sing validated encryption technologies to protect communications and data stored on all devices, including personally-owned devices," "[e]nsuring that remote access servers are secured effectively and kept fully patched," and improving system access security by requiring multi-factor authentication. Investment companies and their directors may also wish to consider adopting certain of these practices to mitigate cybersecurity risks that have developed in response to remote working environments.

OCIE's September 2020 risk alert highlighted "credential stuffing" attacks, which exploit the tendency for people to reuse their passwords across multiple websites and systems, by bad actors who obtain a list of compromised usernames, email addresses and corresponding passwords from the dark web and attempt to log in and gain unauthorized access.[37] OCIE noted that its examinations have revealed an increase in credential stuffing attacks against SEC registrants and that these attacks can result in loss of customer assets or data. OCIE encouraged investment advisers and broker-dealers to review and update their privacy and identity theft policies to address the risk of credential stuffing. This risk alert serves as a reminder to all market participants, including fund directors, to maintain a strong and unique password for all systems, applications and devices and to update those passwords periodically.

While the SEC guidance discussed above does not specifically address fund directors and their personal cybersecurity practices, the SEC's heightened focus on cybersecurity signals that fund directors should pay attention to SEC guidance and consider adopting enhanced cybersecurity practices in order to reduce the risk of a cyber-attack or security breach. Given the pace of its recent alerts on this topic, the SEC will likely continue to issue additional cybersecurity guidance and may seek to cover an expanded group of market participants, including fund directors.

Corporate Director Guidance

Recognizing the importance of cybersecurity, the National Association of Corporate Directors (NACD) has published several editions of a widely-read *Handbook on Cyber-Risk Oversight* that identifies five guiding principles: (1) understanding cybersecurity as a strategic risk; (2) understanding legal implications of cyber risk; (3) providing access to cybersecurity expertise and allowing for adequate time to discuss cybersecurity; (4) managing risk with an enterprise-wide framework; and (5) measuring cybersecurity risks and determining which risks to accept, mitigate, or transfer.[38] Investment companies

and their boards may wish to adopt certain practices based on this guidance for corporate board members, for example: "develop[ing] and adopt[ing] a [board-wide] risk management plan and internal communications strategy."[39]

Fund Policies and Procedures

Director use of email, board portals and other digital technology may be governed by various fund policies and procedures, including the code of ethics, privacy policy, record retention policy, communications policy, cybersecurity policy, information security policy and governance policy, as applicable to the fund company. In many cases, however, fund directors (particularly independent directors) may not explicitly be covered by the funds' policies; alternatively, the policies may be written at a high level and do not address requirements applicable to individual directors. Accordingly, expectations regarding director cyber practices may be communicated by fund management and legal counsel, as part of a new director orientation, a director education session or through other informal communications. As with any policy, a paramount concern is that a policy regarding director communications, record retention or technology be followed and implemented; if directors do not adhere to a fund policy, for example, by continuing to use personal email to discuss fund business, the fund would be better off not adopting a strict policy with respect to these topics.

Whether or not a fund director is explicitly covered by the fund's cybersecurity policy or other compliance procedures, a director's use of email, board portals, cell phones and other electronic devices is governed by the legal duties set forth above, with the duty of care and confidentiality as paramount concerns. In addition to adhering to good cyber hygiene (see discussion below), a director should promptly report to the fund's chief compliance officer or other appropriate fund personnel any cyber breach in which fund or shareholder data may have been compromised. Once reported, the fund can then work with the director to remedy the breach and engage in any required reporting or regulatory documentation or actions.

Enforcement and Litigation Issues

In addition to growing cybersecurity risks, director communications, and the related use of technology, can raise issues in the event of regulatory examinations or lawsuits involving the fund company. If a director communicates fund matters using a personal or another business email address and his or her communications are requested as part of an SEC exam or litigation demand, the document production process will be more difficult (and costly) than if the director had only communicated using a dedicated, fund-provided email address. Specifically, fund directors must be aware of the possibility that using personal email to conduct fund business potentially exposes the director's entire personal email account to review during the discovery process in litigation. Director communications also will be subject to varying, and potentially inconsistent, record retention and destruction practices if directors use personal or other business email addresses for fund business. Corporate directors' personal email and text messages are increasingly included in books and records requests in Delaware courts.[40] In order to mitigate these risks, directors should limit their communications outside of board meetings and avoid taking notes during board meetings. As stated by Daniel Blinka, a shareholder on Godfrey & Kahn's Government Investigations, White Collar and Compliance team, "from a litigation and enforcement standpoint, less is often more."

Cybersecurity Best Practices for Director Communications and Board Materials

Given the continued focus on cybersecurity in the investment industry as well as the rapid adoption of technology over the past year, it is timely and prudent for funds and their directors to consider their

use of technology, including virtual board meeting platforms, digital board book portals, email, texting and personal devices. Funds and directors should be aware of cybersecurity risks attendant to this technology and consider the practices below to mitigate against those risks.

Board Meetings

Because the COVID-19 pandemic caused most board meetings to move to a virtual platform, fund directors (as well as other attendees) should pay particular attention to their personal cyber practices with respect to accessing board meetings and reviewing board meeting materials. The confidential and investment-related nature of the information discussed during board meetings makes virtual meetings of financial services companies, including investment companies, a highly attractive target for cybercriminals.

Whenever a director accesses a board meeting through the Internet, he or she should observe safe Internet practices. For example, a director should not log into a board meeting through the Internet in an unsecured location such as a hotel lobby, airport, or coffee shop. Instead, if a director must log into a board meeting from such a public place, a director should use a MiFi device that should provide a more secure Internet connection. A fund director's passwords for their device or for board book services should be completely unique from the director's other passwords. The passwords should avoid including any personal information and be a minimum of 12 characters.

Use of Video Platforms

At the outset, it is essential for the fund company to vet the video platform on which it hosts board meetings to ensure the platform has strong security. Even the most commonly-used platforms such as WebEx, Microsoft Teams and Zoom face security risks—although platform security generally has improved over the course of the pandemic with respect to Zoom and other commonly-used subscription (as opposed to free) services used by businesses. If a well-vetted platform is used, the board meeting should be encrypted and private. All participants in the meeting should be confirmed before the meeting begins and the participant list should be reviewed and continually monitored throughout the meeting. If an individual calls in to the board meeting, for example, the name of that individual on the phone line should be verbally confirmed.

Meeting attendees also should be aware of the physical environment in which they are participating the meeting. A board member should be in a private area where there is no risk of anyone looking at their device over their shoulder or eavesdropping on the meeting.

Digital Board Book Services

While digital board book services have become more prevalent, there are some cybersecurity risks associated with their use. As with video platforms, it is important to use well-vetted and secure board book portals. A board book portal service may be a high-profile target for a cybercriminal given the sensitive and confidential nature of the information that can be accessed through the board portal service. On the other hand, a reputable board book portal can offer cybersecurity benefits because it can serve as a single, secure repository for board communications, and prevent the loss or misuse of physical board materials. A board portal can also replace the need for separate email communications between fund directors, although the additional step of communicating through the portal may not be convenient or efficient for some directors. Instead of a digital portal, some fund companies use physical board books or electronic PDFs of board materials delivered through a secure portal, such as WebEx, that can mitigate cybersecurity concerns. For those companies that use digital portals, "the cyber risks of major communications can largely be fixed through the board portal, but many times it is the little stuff that gets people in trouble," observes Dennis Connolly,

a shareholder in Godfrey & Kahn's Securities Law practice group, noting the prevalence of business communications via text and personal email.

When accessing a digital board book on a portal, from a cybersecurity perspective, fund directors should try to avoid downloading the board book, although this may not be possible in practice. If the director does download the book, he or she should be aware of the risks related to where that book is saved. If the board book is saved on a device, the device should be encrypted and password protected. Encrypting a device is often as simple as updating the device's security settings to add encryption. If the board book is saved to a third-party cloud, the service should be well-vetted. A strong password should be used and the file should be encrypted. If a board book is printed from a portal, the director should be aware of the physical security of the document and where it is kept and ensure that the hard copy is shredded or returned to the fund company for destruction after the board meeting.

The subject of note taking—whether within the portal, outside the portal electronically or by hand—raises concerns not just related to cybersecurity. Some fund companies have policies related to note-taking that must be followed; fund counsel will likely provide advice in this area. In addition, while a fund director is not an official note-taker for the fund company, any notes that are kept are potentially discoverable in litigation. Therefore, fund directors generally should discard any notes immediately after a board meeting, whether through deletion on the portal or by hand. It is important to keep in mind that notes kept in electronic copy on a fund director's device or in a cloud face the risk of being accessed by a cybercriminal through a cyberattack or security incident.

Use of Personal Email or Devices

As noted above, some directors use a personal email account or device to communicate regarding board activities or even use an email address or device from another business. On the other hand, some fund companies or their investment advisers provide board members with email accounts and devices. If a board member is using a personal email account or a personal device such as a tablet for board business, the director must be aware of hacking risks. Personal email services should be vetted with an eye toward security. Free email services are more at risk compared to corporate provided email accounts due to a lack of built in or default security settings. Directors must be sure to use strong passwords and encrypt any emails that transmit sensitive board materials. Personal emails are also more susceptible to phishing attacks, as personal accounts may lack security filters that apply in corporate email accounts. Such phishing attacks may allow a hacker access to documents on the device and any networks to which that device is connected. A fund director's personal device should be encrypted, maintain up-to-date software, and have anti-virus and firewall protections. Such protections are more easily maintained on corporate devices where software and security updates can be automatically pushed to the device.

Company-provided email addresses and devices mitigate many of the risks discussed above but create additional risks and challenges. If independent directors and their counsel communicate using an email address provided by the investment adviser, privilege, confidentiality and record retention issues may arise. In addition, setting up, maintaining and updating email addresses and devices for outside directors will likely require significant time and resources from the fund company's operational and IT personnel. Moreover, the company will be responsible for overseeing the safety and security of devices used by outside directors, in addition to their own personnel, and some fund companies may view this as crossing the line into a director's personal data practices. As one fund company executive stated, "the more you provide, the more you have to oversee—that's the rub." And from a practical perspective, fund directors may have a hard time pivoting from the familiarity and convenience of using personal emails and devices.

Post-Meeting Best Practices

Once a board meeting is over, directors should follow any document retention policies, which may be part of a formal record retention policy or guidelines communicated more informally to the director. Typically, best practices include shredding or returning hard copies of information provided for the board meeting, and/or deleting any electronic files with material from the meeting. It is important for fund directors to recall that board meeting recordkeeping is the responsibility of the fund company, and not the individual responsibility of fund directors.[41] Accordingly, there is no need for a director to save personal copies of board books or other handouts from the meeting and indeed, doing so may create risk.

What to Do in Case of a Breach?

Unfortunately, even if all of the best cyber practices are followed, there is no guarantee that a security incident will not happen—a director's email account may be hacked or a board meeting may experience a breach. If a security incident is suspected or does occur, whether that be unauthorized access to board-related emails or board materials, it is essential that the director immediately notify the chief compliance officer or other appropriate contact at the fund company, so that the company may initiate its incident response plan and work quickly to mitigate any potential harm. If an attack is suspected, determining whether the hacker still has access to confidential information or documents and then shutting that access down as quickly as possible is key to mitigating harm to the fund. In the case of a hacker accessing an email account, the fund company will need to know if harmful emails were sent from that inbox to fund personnel or shareholders to try to cut off any spread of malicious emails that may allow the hacker access to other individuals' computers or networks. Time is of the essence in responding to a potential cyberattack.

Indemnity and Insurance Considerations

If a fund director or the fund incurs a loss due to a cyber breach, the director should be indemnified under the fund's governing documents, assuming the director did not engage in bad faith or disabling conduct. Funds typically indemnify their directors to the fullest extent permitted by law against liability incurred as a result of their service as a director.[42] Errors and Omissions (E&O)/Directors and Officers (D&O) liability insurance is the typical mechanism for ensuring the indemnification provisions of the fund's governing documents should a fund director incur any losses and expenses as a result of their position as a director.[43] While coverage under E&O/D&O liability insurance varies by policy and the insurer, E&O/D&O liability insurance generally pays for liabilities arising from acts taken by the director in their official role, including breach of fiduciary duty and negligence.[44] According to Noble Powell, Managing Director and Practice Leader at Asset Management Insurance, the fund's D&O insurance policy should respond to any claims made with respect to a director's conduct, regardless of whether the conduct was carried out through a personal email address or personal device. Fund directors will generally be covered under E&O/D&O liability insurance for their conduct if there is no specific exclusion under the policy for certain allegations related to fund directors' fiduciary duties or negligence.

Funds also may purchase additional, specialized liability insurance policies such as excess independent director liability insurance and cybersecurity insurance. The SEC's Division of Investment Management has encouraged funds to consider whether it is necessary or appropriate for a fund to obtain cybersecurity insurance.[45] The most common cyber liability insurance is a breach response policy, which provides coverage for damages incurred after a cyber breach has occurred, such as breach or loss of data, business interruptions, loss of customers' personally identifiable information, reputational harm expenses, ransom costs and regulatory penalties or fines. Standalone cybersecurity policies tend to be rarely purchased by fund boards, though fund boards may choose to maintain a specialized cybersecurity policy or be jointly added to the cybersecurity

policy of the fund's investment adviser.[46] However, it is unlikely that fund directors will trigger coverage under any specialized cybersecurity policy because a fund director's exposure to cyberattacks or security breaches is, as stated by Mr. Powell, "vicarious at best" since fund directors are not involved in the day-to-day management of the fund. Investment advisers, on the other hand, do face cyber exposure given their role in the day-to-day management of the fund, and therefore, it is more common for advisory firms to obtain specialized cybersecurity policies. Fund directors should work with the fund's insurance broker or legal counsel to determine whether the fund's insurance policy provides coverage for losses in the event of a cyberattack or cybersecurity breach and whether it is necessary for fund directors to be afforded coverage under any cybersecurity insurance policy.

Conclusion

The Forrester Consulting study discussed in the introduction stated, "[w]e found that board members and governance professionals don't associate their own communication practices with the company's cybersecurity posture."[47] Fund directors are increasingly dependent on technology, both for communication and the conduct of meetings, and their personal cyber practices may indeed create risk for the funds they oversee. As of the date of the completion of this article, the SEC has not yet terminated its exemptive relief regarding in person board meetings under the 1940 Act.[48] While many boards will resume meeting in person on a regular basis as soon as practical, others may adopt a hybrid model in which some board meetings are conducted via video platform and others are held in person. Accordingly, it is likely that cyber issues faced by directors both individually and in overseeing the fund will continue to grow. Directors may wish to use their experiences with technology over the past year (or more) to work with counsel and fund management to refine and enhance both individual and fund-level cyber practices.

Ms. Campbell is a member of the Data Privacy & Cybersecurity practice group at Godfrey & Kahn, S.C., where her practice focuses on advising clients with respect to cybersecurity, data privacy and data breach response and remediation. **Ms. Drought** is a shareholder, and **Ms. Johnson** is an associate, in the Investment Management practice group at Godfrey & Kahn, S.C. where they specialize in advising investment companies and their boards with regard to regulatory, governance and general corporate matters.

NOTES

1 *See*, *e.g.*, Mutual Fund Directors Forum, "Board Oversight of Cybersecurity" (Nov. 2015), *https://www.mfdf.org/docs/default-source/default-document-library/publications/white-papers/cybersecurity.pdf?sfvrsn=8d3e4df3_4*.

2 SEC, Div. of Examinations, 2021 Examination Priorities at 24, *https://www.sec.gov/files/2021-exam-priorities.pdf*; SEC, Div. of Inv. Mgmt., IM Guidance Update: Cybersecurity Guidance, No. 2015-02 (Apr. 2015), *www.sec.gov/investment/im-guidance-2015-02.pdf*.

3 Forrester Consulting, "Directors' Digital Divide: Boardroom Practices Aren't Keeping Pace with Technology" (Oct. 2018), *https://diligent.com/wp-content/uploads/sites/5/2018/11/UK-Diligent-Global-Report-Forrester-Directors-Digital-Divide-Boardroom-Practices.pdf*. This survey included executives, directors, leaders and staff of private companies, public companies, not for profit organizations and governmental entities.

4 Maggie Miller, "FBI sees spike in cyber crime reports during coronavirus pandemic," *The Hill* (Apr. 16, 2020), *https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic*.

5 ABA Fed. Regulation of Securities Comm., Fund Directors Guidebook § 3 (4th ed. 2015); Ellen R. Drought & Pamela M. Krill, "Fiduciary

Duties of Directors of Registered Investment Companies," *Inv. Law.*, May 2017, *www.gklaw.com/NewsUpdatesPressReleases/Fiduciary-Duties-of-Directors-of-Registered-Investment-Companies.htm*.

6 William M. Lafferty, Lisa A. Schmidt, and Donald J. Wolfe, Jr, "A Brief Introduction to the Fiduciary Duties of Directors Under Delaware Law," 116 *Penn. St. L. Rev*. 837 (2012), *http://www.pennstatelawreview.org/116/3/116%20Penn%20St.%20L.%20Rev.%20837.pdf*.

7 Steven B. Stokdyk and Joel H. Trotter, "Maintaining Director Confidentiality," Harvard Law School Forum on Corporate Governance (Feb. 15, 2016), *https://corpgov.law.harvard.edu/2016/02/15/maintaining-director-confidentiality/*.

8 Drought & Krill, *supra* n.5, at 1 n.4.

9 *Id.*, *supra* n.5.

10 *See* Mutual Fund Directors Forum, "Role of the Mutual Fund Director in the Oversight of the Risk Management Function" (May 2020), *https://www.mfdf.org/docs/default-source/default-document-library/publications/white-papers/mfdfriskoversightpaper-may2020f.pdf?sfvrsn=95c2cce4_4*.

11 *Id.*; Drought & Krill, *supra* n.5, § 3.

12 Board Oversight of Cybersecurity, *supra* n.1; Drought & Krill, *supra* n.5.

13 *See* 15 U.S.C. § 6801 et seq.; 23 NYCRR 500. The number of state specific laws with cybersecurity requirements are growing. Laws in California and Massachusetts are prime examples. The California Consumer Privacy Act (CCPA) and the more recent California Privacy Rights Act (CPRA) also contain data security obligations. *See generally* CCPA, Cal. Civ. Code § 1798.100 et seq.; CPRA, Cal. Civ. Code § 1798.150(a)(1). While personal information collected pursuant to GLBA is currently exempted under CCPA, funds should be aware that to the extent they maintain other personal information not subject to GLBA, such as marketing information for potential clients, there may be cybersecurity obligations under California state law. *See* CPRA, Cal. Civ. Code § 1798.145(e). Massachusetts requires entities that handle the personal information of Massachusetts residents to have certain cybersecurity measures in place, including a written information security program. 201 CME 17. In the case of financial institutions, such written information security program must comply with GLBA requirements. *Id.*

14 *See* 16 C.F.R. §§ 313, 314.

15 23 NYCRR Part 500.

16 *See* 16 C.F.R. § 313.

17 *See* 16 C.F.R. § 314.

18 *Id.*, § 314.1.

19 *Id.*, § 314.2.

20 *Id.*, § 314.3.

21 *Id.*

22 23 NYCRR 500.

23 23 NYCRR 500.2.

24 *Id.*

25 23 NYCRR 500.14.

26 In its 2021 Examination Priorities, *supra* n.2, the Division of Examinations noted that "the increase in remote operations in response to the pandemic has increased concerns about, among other things, endpoint security, data loss, remote access, use of third-party communication systems, and vendor management." 2021 Examination Priorities at 24.

27 IM Guidance Update: Cybersecurity Guidance, *supra* n.2.

28 SEC, Office of Compliance Inspections and Examinations, Cybersecurity and Resiliency Operations (Jan. 2020), *https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf*.

29 *Id.*

30 OCIE, Cybersecurity: Ransomware Alert (July 10, 2020), *https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf*.

31 *Id.*

32 *Id.*

33 *Id.*

34 OCIE, Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers (Aug. 12, 2020), *https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf*.

[35] *Id*.

[36] *Id*.

[37] OCIE, Cybersecurity: Safeguarding Client Accounts against Credential Compromise (Sept. 15, 2020), *https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf*.

[38] Larry Clinton, Nat'l Ass'n of Corporate Directors, "Cyber-Risk Oversight 2020, Key Principles and Practical Guidance for Corporate Boards" (Feb. 2020), *https://tinyurl.com/4wksv49t*.

[39] *Id*. at 27.

[40] Jennifer Williams-Alvarez, "Investors are Getting Directors' Personal Texts and Emails," *Agenda*, Mar. 19, 2021.

[41] *See* Rule 32a-1 under the Investment Company Act.

[42] Drought & Krill, *supra* n.5, §16.

[43] *Id*.; Mutual Fund Directors Forum, "Practical Guidance on Director and Officer Insurance for Fund Independent Directors" (Jan. 2018), *https://www.mfdf.org/docs/default-source/default-document-library/publications/white-papers/d-o.pdf?sfvrsn=e091751c_0*.

[44] *Id*.

[45] IM Guidance Update: Cybersecurity Guidance, *supra* n.2.

[46] Practical Guidance on Director and Officer Insurance for Fund Independent Directors, *supra* n.43. According to Mr. Powell, a fund board can generally be added to an adviser's cybersecurity policy for a minimal cost.

[47] *See* Forrester Consulting, *supra* n.3, at 1.

[48] *See* Investment Company Act Release No. 33897 (June 19, 2020), *https://www.sec.gov/rules/exorders/2020/ic-33897.pdf*.