Risk Management in the Digital Age

Mobile Computing, Cloud Computing and Social Media

ICIMutual
The safest decision you can make

Risk Management in the Digital Age: Mobile Computing, Cloud Computing and Social Media

Introduction

Recent years have witnessed significant developments in cyber technologies, most notably (1) the evolution of "**mobile computing**"; (2) the emergence of "**cloud computing**"; and (3) an exponential growth in the use of "**social media**." For the fund industry, these technologies are affecting—and could eventually transform—how electronic information is communicated, collected, stored, and processed by businesses and individuals. These technologies also present risk management challenges.

These new technologies are complex and rapidly evolving, and the terminology used in describing them can be confusing. Even for advisory personnel who are generally conversant in cyber issues, the sources and nature of the risks presented by these technologies may not be readily apparent. Fund advisers may therefore find it useful to have access to resources that can assist their personnel in developing a better understanding of these new technologies and their attendant risks.

This study is designed to serve as such a resource. Geared for non-experts, this study provides a general introduction to: (1) mobile computing, cloud computing, and social media, (2) the financial, legal, and reputational risks associated with their use, and (3) approaches that may assist fund groups in managing these risks. In addition, the study provides an overview of insurance products that may assist in mitigating the exposures associated with various cyber risks.

This study is directed primarily towards senior management and towards legal, compliance, and other personnel with responsibility for assessing and managing technology-related risks for fund groups.[1] The study is intended to facilitate discussion between such individuals, on the one hand, and information technology personnel and other specialists, on the other, and thereby to assist investment advisers in identifying various types of risks associated with these new technologies, and in developing and implementing appropriate techniques and procedures for managing them. Independent fund directors may also find the study useful in connection with their oversight of risk management.

The contents of this study reflect interviews with selected fund groups, consultation with counsel and other industry experts with specialized knowledge regarding cyber technologies, and review of publicly available materials. Nothing in this study should be considered legal advice; rather, readers should look to their counsel for such advice. Moreover, this study is not intended to, and does not, recommend any single approach or set of "best practices." Indeed, in the area of managing cyber technology risks, one-size-fits-all standards are generally not practical or advisable, given the diversity of the industry and of risk management processes and techniques. Effective management of cyber technology risks will depend on many factors particular to each fund group, including the nature and scope of the group's use of such technologies, the structure and culture of the group, and the extent of the group's reliance on third-party service providers.

---

[1] While this study focuses on risks and risk management approaches for registered investment companies ("funds"), the topics and techniques discussed may also be relevant to an adviser's private account management business.

Executive Summary

Fund groups have long used computer-based technology for the communication, collection, storage, and processing of information, and have long sought to manage the risks associated with the use of such technology. Their efforts have largely focused on safeguarding identified categories of confidential or otherwise sensitive information (see inset at right)—as well as protecting related computer systems and applications—against various cyber threats. For fund groups, the failure to adequately safeguard sensitive information against such threats may lead to: (1) financial damage, both direct (e.g., losses resulting from the misappropriation of proprietary or client assets) and indirect (e.g., costs and expenses associated with restoring affected computer systems, applications, and information); (2) legal damage, in the form of private lawsuits and/or regulatory enforcement actions (e.g., for violations of privacy laws and regulations); and (3) reputational damage (e.g., arising from data breaches that lead to unauthorized use or dissemination of sensitive information about shareholders, clients, or employees).

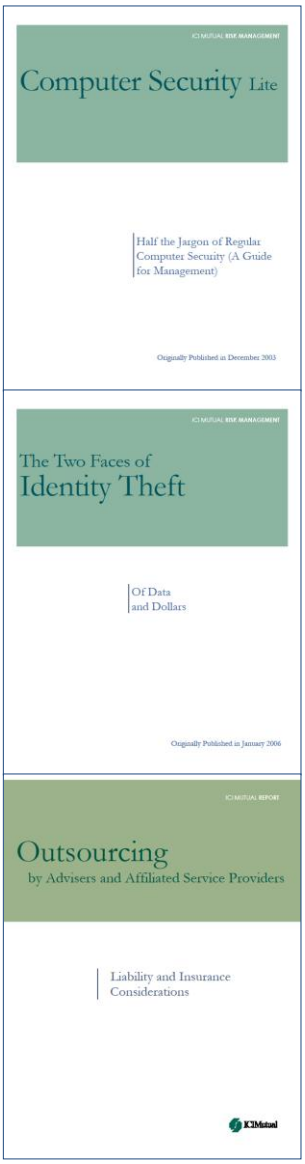
Categories of Confidential or Otherwise Sensitive Information

- ***Shareholder information*** – This category includes account information, personal financial and other information about shareholders, and passwords and other account access data.
- ***Investment management information*** – This category includes portfolio holdings, trading data, and fund accounting information, as well as intellectual property, such as investment strategies or methodologies and proprietary trading models.
- ***Corporate records and other information relating to internal operations*** – This category includes corporate account information, details about corporate operations, and personal information about officers and employees, including payroll, financial, and medical information.

Recent years have witnessed exponential growth in the use of **mobile computing** and **cloud computing** by businesses and individuals, including fund groups and fund shareholders. Section I of this study examines these two technologies. The term "mobile computing," as used in this study, refers to technologies that permit the transmission, collection, processing, and/or storage of electronic information from wherever a user may happen to be. The term thus encompasses the use of smartphones, laptops, tablets, or similar devices by fund shareholders, third-party providers, and/or employees to access fund groups' computer networks (including their websites or social media sites), as well as the use by such parties, and by fund groups themselves, of "wireless" computer networks and associated hardware (such as wireless access points and routers). The term "cloud computing," as used in this study, refers to technologies that permit businesses or other users to "outsource" the storage of electronic information to offsite data centers that are typically owned and operated by third-party vendors. These vendors may also provide an array of user services beyond data storage (e.g., data processing, software applications, user authentication, encryption, and software maintenance).

The two technologies—mobile computing and cloud computing—represent a significant evolution in how sensitive information is electronically communicated, collected, stored, and processed. For the most part, however, the risks to fund groups associated with the use of these two technologies are not fundamentally new; rather, the risks tend to be of the same basic types (e.g., fraudulent transactions, hacking incidents) that have long been associated with the use of computer-based technologies and/or with the "outsourcing" by fund advisers or their affiliates of specialized functions to unaffiliated third-party vendors. As a result, in addressing risks associated with mobile computing and cloud computing, fund groups have tended to build upon their existing risk management programs, making modifications as appropriate in light of the unique aspects of the two technologies.

Recent years have also witnessed exponential growth in the use of Internet-based **social media** by businesses and individuals, including fund groups and fund shareholders. Section II of this study examines this development. For fund groups, the use of social media represents a significant evolution in how "public" information (i.e., non-confidential information) is made available to the public at large, not only by fund groups themselves, but also by their employees, shareholders, or other third parties. Cyber incidents involving such "public" information can potentially result in financial damage for fund groups. But, perhaps more problematic for them, is the potential for business disruption and/or reputational damage. Moreover, the use and transmission of "public" information via social media may implicate various laws and regulations, and thereby heighten regulatory risk. As a result, in addressing risks associated with social media, fund groups have tended to focus on monitoring the use of these media (both internally and externally), and on staying current with regulatory developments.



The growth and evolution of mobile computing, cloud computing, and social media underscore the value to fund groups of understanding and evaluating the nature and scope of insurance protections that may be available to address various cyber risks. Section III of this study surveys these protections. As discussed in that section, many investment company blanket bonds and directors and officers/errors and omissions liability insurance policies provide a limited degree of cyber coverage. However, these products are not designed to provide broad coverage against cyber risks. By contrast, specialized cyber insurance policies (generally issued on a stand-alone basis) are often specifically designed to address a wide array of cyber exposures.

This study assumes familiarity with basic computer technology risks and risk management techniques. For a general introduction to the risks associated with computer-based technologies in the fund context, and to the broad components of effective programs for managing these risks, readers may wish to consult ICI Mutual's prior risk management study, entitled *Computer Security Lite* (2003), which, despite its publication date, remains relevant today. Other relevant background and guidance may be found in two additional ICI Mutual risk management studies, entitled *The Two Faces of Identity Theft* (2006) and *Outsourcing by Advisers and Affiliated Service Providers* (2008).

Mobile and Cloud Computing: Safeguarding Sensitive Information

Recent years have witnessed significant growth in the use of mobile computing and cloud computing by businesses and individuals, including fund groups and fund shareholders. This growth has brought new attention to attendant cyber risks faced by fund groups, and to the risk management programs used in addressing and managing these risks. This section provides a general introduction to these technologies, to the key risks to fund groups associated with their use, and to approaches that may assist fund groups in managing these risks.

Mobile Computing

The term "mobile computing," as used in this study, refers to technologies that permit the transmission, collection, processing, and/or storage of electronic information from wherever a user may happen to be. The term thus encompasses the use of smartphones, laptops, tablets, or similar devices by fund shareholders, third-party providers, and/or employees to access fund groups' computer networks (including their websites or social media sites), as well as the use by such parties, and by fund groups themselves, of "wireless" computer networks and associated hardware (such as wireless access points and routers). An array of "mobile" activity is thus included within the concept of mobile computing—e.g., the fund shareholder who checks her fund group's mobile website via her smartphone, the employee working from home who accesses his fund group's network via his laptop or tablet, and the employee of a third-party provider who uses a laptop to obtain authorized access to a fund group's network.

For the most part, the risks to fund groups associated with mobile computing are not fundamentally new; rather, the risks tend to be of the same basic types (e.g., fraudulent transactions, hacking incidents) that have long been associated with the use of computer-based technologies. As a result, in addressing risks associated with mobile computing, fund groups have tended to build upon their existing cybersecurity risk management programs, making modifications as appropriate in light of the unique aspects of the technologies. In evaluating whether and how to make such modifications, it is useful to consider separately the risks associated with (1) **mobile devices** (e.g., laptop computers, tablets, smartphones), (2) **insider access** (i.e., the use of wireless and/or wired connections to fund group networks by employees and other trusted users), and (3) **public access** (i.e., the use of fund groups' full websites, mobile sites, and/or mobile applications by shareholders, potential shareholders, and other members of the public).

MOBILE DEVICES

The devices used for electronic communication have become more portable, more powerful, and more convenient. Transactions and other communications that were once typically effected by using a hard-wired

NASA: "Your cell phone has more computing power than the computers used during the Apollo era."

Source: http://www.nasa.gov/audience/foreducators/diypodcast/rocket-evolution-index-diy.html

desktop computer can now be accomplished by laptop computers and other wireless devices, such as netbooks, tablet computers, and smartphones.

Not surprisingly, given the significant overlap in their functionality and features, mobile devices and traditional desktop computers share many of the same basic vulnerabilities to cyber threats. However, the very "mobility" of such devices gives rise to certain new and/or heightened vulnerabilities. Key risks associated with mobile devices include:

- ***Loss or Theft:*** The size and portability of mobile devices increase the likelihood of loss or theft.[2]

- ***Improper or Incomplete Disposal of Residual Information:*** Mobile devices tend to be replaced or upgraded more often than traditional desktop computers. As a result, it may be more likely for sensitive information—or the means to access such information—to be inadvertently left on such devices.

- ***Limited Security Features:*** Mobile devices and the apps designed for mobile devices often emphasize user convenience over security considerations. In that regard, they typically lack the range of integrated security features commonly found on desktop computers.[3]

- ***Use of Untrusted Networks:*** Mobile devices are frequently used in locations outside of the workplace (e.g., employees' homes, coffee shops, hotels, conferences) and, as a result, often rely on external (sometimes public) networks for Internet access. These external networks are not necessarily trustworthy (i.e., sufficiently secure).[4] The use of mobile devices in public locations also presents the risk of so-called "shoulder surfing" (i.e., that someone will obtain sensitive information by surreptitiously reading from an employee's mobile device).

- ***Susceptibility to Malware:*** Mobile devices may be susceptible to attack by a wide variety of malware, which may be introduced via communications services (e.g., text messaging, WiFi, broadband Internet, cellular data), via synchronization with a desktop computer or network, via e-mail or web browsing, or via infected storage media.

- ***Less Robust Safeguards:*** The adoption of mobile devices used in the work environment often takes place informally or in a piecemeal manner.[5] As a result, an IT department may not recognize all active mobile devices (e.g., personal mobile devices) as part of its infrastructure nor treat them accordingly.

---

[2] *See* Cloud Security Alliance, *Data Loss from Missing Mobile Devices Ranks as Top Mobile Device Threat*, Oct. 4, 2012, https://cloudsecurityalliance.org/csa-news/data-loss-mobile-ranks-top-threat-enterprises/.

[3] *See* Ashlee Vance, *Gadgets Bring New Opportunities for Hackers*, Dec. 26, 2012, http://www.nytimes.com/2010/12/27/technology/27hack.html.

[4] *See* Analisa Nazareno, *How free Wi-Fi can put you at risk*, Nov. 8, 2011, http://money.msn.com/identity-theft/how-free-wi-fi-can-put-you-at-risk-credit-cards.aspx; *see also* Wall Street Journal, *Almost 80% Believe Free Wi-Fi Can Lead to Identity Theft, Study Finds*, Oct. 18, 2012, http://online.wsj.com/article/PR-CO-20121018-903577.html.

[5] *See* Ellen Messmer, *Young employees say BYOD a "right" not "privilege"*, June 19, 2012, http://www.networkworld.com/news/2012/061912-byod-20somethings-260305.html.

With the rapid proliferation of mobile devices in the workplace (both in number and variety of devices), fund groups are focusing substantial time and resources on developing and enforcing enterprise-wide security policies to specifically address the risks presented by mobile devices to their computer networks and data. In particular, fund groups frequently seek to heighten (or otherwise buttress) protections in the areas of authentication of users, protection of data, and limitations on users' ability to configure mobile devices (see inset). A more complete discussion of the compliance and risk management approaches relevant to mobile computing, including mobile devices, begins on page 13.

Securing Mobile Devices

Common steps taken to secure mobile devices include the following:

- Requiring authentication (e.g., password or passcode) for both the user and the device before accessing an organization's computer network
- Remotely locking access or "wiping" the device (deleting stored data) if lost or stolen
- Using strong encryption for both data communications and data storage
- Limiting access to device hardware (e.g., digital camera, removable storage) and software (e.g., application installation services)
- Restricting applications which may be installed by the user on the device
- Managing wireless network interfaces (e.g., Wi-Fi, Bluetooth)
- Automatically monitoring and reporting when security policy violations occur

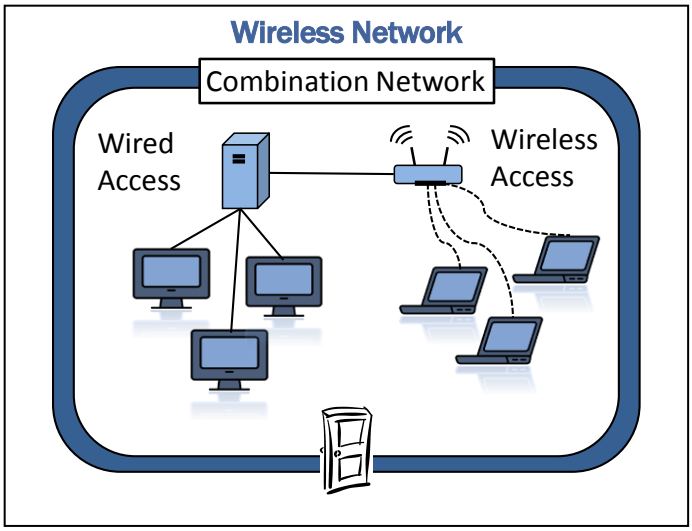
See, e.g., Guidelines for Managing and Securing Mobile Devices in the Enterprise, Special Publication 800-124 Revision1 (Draft), National Institute of Standards and Technology, Information Technology Laboratory, July 2012, http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf.

INSIDER ACCESS

Broadly speaking, electronic access by insiders (i.e., employees or other trusted users) to a fund group's computer network may take place from within the computer network itself (i.e., "internal" access), or from outside the network (i.e., "remote" access). In either case, electronic access may be effected through wired connections, wireless connections, or a combination of both. The trend toward mobile technology has highlighted security risks associated with (1) internal access effected through wireless connections (i.e., "**wireless networks**" in the workplace), and (2) insider access effected **remotely** (i.e., from outside the workplace, often through the use of mobile devices).

Wireless Networks

Until relatively recently, fund groups largely relied on wired connections to build their internal computer networks (also known as local area networks, or LANs). In so doing, fund groups used wires or cables (e.g., Ethernet cables) (1) to *physically* connect desktop computers within the network to other network resources such as file servers or printers, and (2) to *physically* connect their computers networks to the outside world (including the Internet, branch offices, or service providers.)[6]



[6] A wired network can be protected by both physical and logical barriers. Physical barriers include limiting network access to employees (or other authorized users) within the confines of a building or suite of offices. Logical barriers include conventional security measures, such as software-based or hardware-based firewalls, to prevent unauthorized access to or from a private network.

As the name suggests, **wireless networks** (also known as wireless local area networks, or WLANs)[7] typically rely on radio waves (rather than on wires) to permit users to connect to each other and to the outside world.[8] This configuration provides users with the flexibility to move around physically within a local coverage area and still be connected to the computer network (and to the Internet). Wireless access may additionally offer cost advantages to a fund group as well as increased flexibility when responding to changes in IT infrastructure needs (e.g., less network cabling and fewer ports may be required). Wireless networks can also be found in use outside the corporate context, in the form of *private* wireless networks (e.g., at the homes of employees or shareholders) and *public* wireless networks (e.g., WiFi hotspots in coffee shops, libraries, hotels, and airports).[9]

Wireless networks have many of the same risks as wired networks, but may also present greater risk in certain areas.[10] Key risks associated with wireless networks include:

- ***Unauthorized Network Access Without Physical Access:*** Wireless signals may be broadcast in an open and detectable manner and will often travel well beyond the organization's physical security perimeter. As a result, this may heighten the risk that unauthorized users (who may not even be on an organization's property) may gain access to network resources, personal shareholder information, and/or proprietary data.

- ***Exposure of Data in Transit:*** A wireless connection that does not adequately secure the integrity of wireless transmissions could expose information and data to unauthorized access and result in the manipulation and/or corruption of such data and information. For example, in certain instances, information may be transmitted in clear text (i.e., unencrypted) and may therefore be readily intercepted or may be susceptible to manipulation. Moreover, such interception or manipulation could go undetected by the sender and recipient.

- ***Loss of Network Availability:*** An attacker could stop authorized users from using a fund group's computer network by exploiting vulnerabilities in a wireless access point to render the system inoperable, by jamming the radio frequency used by the network, or by flooding the network with traffic (i.e., denial-of-service attacks) – potentially reducing the group's ability to provide certain services to shareholders.[11]

---

[7] Wireless networks are also commonly referred to as "wireless campuses" or "WiFi networks" (referring to the trademarked name of a popular wireless technology).

[8] Infrared technology, satellite signals, cellular service, and free-space optics can also be used to connect devices wirelessly to each other and/or the Internet.

[9] While private wireless networks may be configured to have strong encryption, public wireless networks (such as WiFi hotspots) are generally *not* encrypted. *See* note 10 *infra*.

[10] *See* Shirley Radack, ed., *Security for Wireless Networks and Devices*, Mar. 2003, NIST, Information Tech. Laboratory, http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm.

[11] *See*, *e.g.*, Sheila Frankel, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, pp. 3-6, Special Publ'n 800-97, Feb. 2007, NIST, Info. Tech. Lab., http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf.

Notwithstanding advances in wireless security, wireless networks are generally viewed more susceptible to intrusion than their wired counterparts. Consequently, fund groups frequently seek to strengthen protections in the areas of data security, user authentication, and security monitoring (see inset). A more complete discussion of compliance and risk management approaches relevant to mobile computing, including wireless networks, begins on page 13.

Securing Wireless Networks

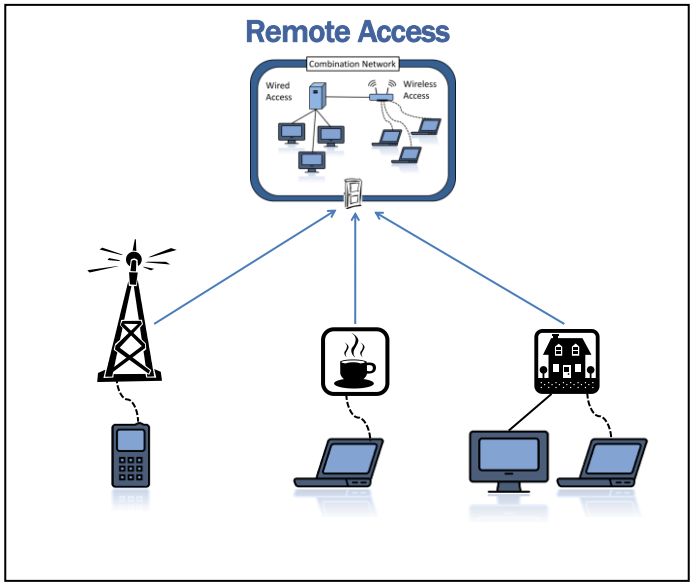
Common steps taken to secure wireless networks include the following:

- Using strong encryption for wireless network traffic
- Restricting access to pre-approved devices (often known as MAC address filtering)
- Performing both attack monitoring and vulnerability monitoring to support wireless network security
- Conducting regular periodic technical security assessments for wireless networks
- Standardizing security configurations for common wireless network components, such as client devices and access points

See, e.g., Murugiah Souppaya and Karen Scarfone, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, Special Publication 800-153, National Institute of Standards and Technology, Information Technology Laboratory, Feb. 2012, http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf.

Remote Access

Many fund groups have long permitted some type of remote access to their internal computer networks, including, for example, in the context of "telework" programs (where employees access networks from home or while traveling). The level of network access provided to remote users can vary significantly, with access in some cases being substantially the same as would be permitted onsite. While remote access need not be effected through wireless connections (or through mobile devices), it is not uncommon for fund groups to permit employees (and in some cases, service providers) a degree of access to their internal computer networks in this way.



Key risks associated with the use of remote access arrangements include:

- ***Unauthorized Access:*** Confirming the identity of a user seeking access to a computer system is a standard part of an effective computer security program. This so-called authentication process is of particular importance with respect to remote users.

- ***Exposure of Data in Transit:*** The protection of data transmitted between a user's computer and a fund group's computer network becomes more difficult in the context of remote access. Nearly all remote access is established over the Internet and often involves the use of external networks, whose security is generally outside of the control of the group and may be inadequate.

- ***Inadequacy of Physical Security Controls:*** The devices (whether wired or wireless) used to access a group's internal computer network are outside of the group's control and are at risk of being lost, stolen, or otherwise accessed by an unauthorized party.

- ***Connection of Infected Devices to Internal Networks:*** The devices used for remote access may be infected with malware that could spread once the devices are connected to internal computer networks

Many of the steps that may be taken to secure mobile devices and wireless networks may also apply to remote access. Fund groups typically take a variety of steps in, for example, the areas of data protection, authentication of users, and access limitations on users (see inset) to ensure the security of remote access to their networks. A more complete discussion of compliance and risk management approaches relevant to remote access begins on page 13.

Securing Remote Access

Common steps taken to secure remote access include the following:

- Using strong encryption in transmission for remote access
- Requiring the use of authentication tokens or other enhanced authentication techniques
- Creating virtual private networks (or VPNs, which allow private communications to be transmitted over the Internet in an encrypted "tunnel")
- Allowing access only through remote desktop software (such as Citrix or GoToMyPC)
- Limiting the scope of access to network data and applications
- Conducting regular periodic technical security assessments for the organization's wireless networks devices and access points

See, e.g., Murugiah Souppaya and Karen Scarfone, *User's Guide to Securing External Devices for Telework and Remote Access*, Special Publication 800-114, Nat'l Inst. of Standards and Tech., Information Tech. Laboratory, Nov. 2007, http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf; Karen Scarfone, *Guide to Enterprise Telework and Remote Access Security*, Special Publication 800-46 Revision 1, Nat'l Inst. of Standards and Tech., Information Tech. Laboratory, June 2009, http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf.

PUBLIC ACCESS

Over the years, fund groups have established a variety of means by which shareholders, potential shareholders, and other members of the public may engage in electronic communications with the fund groups. In recent years, these have included Internet-based connection points, such as **full websites**, **mobile websites**, and/or **mobile applications** ("apps").

Today, virtually all fund groups have full websites. While traditional fund websites are well-suited for users with large computer monitors and reasonably fast Internet connections, these full websites may be

E-mail Communication

E-mail is a common form of business communication, whether between businesses or between businesses and their customers (or shareholders). In some cases, these communications may include confidential or otherwise sensitive information.

For fund groups, e-mail communications may present serious security concerns. It is not uncommon for e-mails to include viruses or other malware. Moreover, e-mails may be transmitted in plain text (i.e., not encrypted) and they can be at risk of being intercepted (or even altered) en route. It is also relatively easy to masquerade e-mails such that they appear to have originated from someone other than the true sender.

These vulnerabilities may be mitigated in a number of ways, including maintaining up-to-date antivirus and anti-malware protection, encrypting the content of e-mails, using cloud servers to host sensitive content, and transmitting e-mail over encrypted channels (e.g., using the so-called transport layer security (TLS)). While these mitigation techniques may be implemented relatively easily in business-to-business communications, implementing such techniques in e-mail communications with shareholders may present more challenges.

Accordingly, fund groups may wish to consider how e-mail communications are being used, and whether additional security controls are warranted (e.g., if shareholders are permitted to give purchase or sale orders by e-mail).

In addition to issues with e-mail communications, fund groups are likely to face the same or similar issues with texting or instant messaging, which may be used for business communications.

cumbersome, slow, and difficult to navigate for users on smaller, mobile devices (which may often have relatively slow Internet connections). As a result, many fund groups also create mobile websites (which are optimized for use on mobile devices) and/or mobile apps (which are smartphone applications that provide some or all of the functionality of the full websites).[12] The variety of mobile devices used for electronic communication has also driven the development by fund groups of different means of accessing their online services, as fund groups seek to accommodate various flavors of smartphones and tablets that use different platforms (i.e., Android, BlackBerry, iOS, or Windows Phone).

Key risks associated with providing the public with new forms of electronic access to fund groups and/or their services include:

- ***Security and Privacy:*** For many fund groups, security and privacy are the chief concerns in developing mobile websites and apps. Mobile apps in particular may present special challenges in this regard.[13] For example, many mobile apps may expose data (including personal or other confidential information), which may then be obtained by other, unrelated mobile apps.

- ***Operational Errors:*** Developing new points of connection may lead to increased administrative and operational issues. Personnel with expertise in full website development may be less versed in developing mobile websites or apps. Moreover, it may be more difficult and time-consuming to ensure that all access points are properly maintained and updated.

Fund groups typically consider a variety of steps to secure mobile websites and mobile apps (see inset). A more complete discussion of compliance and risk management approaches relevant to public access to fund groups begins on page 13.

Securing Mobile Websites and Mobile Apps

Ensuring the security of mobile websites and mobile apps involves consideration and understanding of numerous factors, including:

- The idiosyncrasies of the specific platform(s) (e.g., Android or iOS) on which the website will be accessed or the app will be used
- The extent to which sensitive information will be stored on the mobile devices
- The encryption of information both stored on and transmitted by the mobile devices

See, e.g., Secure Mobile Application Development Reference, Denim Group, 2011, http://www.denimgroup.com/media/pdfs/MobileDevReference.pdf (providing guidelines for developing secure mobile apps).

---

[12] Beagan Wilcox Volz, *Franklin Templeton Latest to Go Mobile*, Ignites, Dec. 8, 2011, http://www.ignites.com/c/285351/33631/Franklin_Templeton_Latest_to_Go_Mobile?referrer_module=searchResults&module_order=14&highlight=franklin+mobile (four of the 10 largest fund firms do not offer mobile access or mobile apps); Emile Hallez, *Firms Push Out Mobile Apps in Bid to Woo 401(k) Savers*, Ignites, June 13, 2012, http://www.ignites.com/c/368892/41852/Firms_Push_Out_Mobile_Apps_in_Bid_to_Woo_401k_Savers_?referrer_module=searchResults&module_order=1&highlight=bid+to+woo (major retirement plan providers are releasing mobile apps to investors); Jackie Noblett, *Funds Scramble to Keep Pace With Mobile Trends,* Ignites, June 29, 2011, http://www.ignites.com/c/215462/26972/Funds_Scramble_to_Keep_Pace_With_Mobile_Trends?referrer_module=searchResults&module_order=3&highlight=keep+pace+with+mobile (major fund groups are launching mobile apps).

[13] *See, e.g.*, *Secure Mobile Application Development Reference*, Denim Group, 2011, http://www.denimgroup.com/media/pdfs/MobileDevReference.pdf (providing guidelines for developing secure mobile apps).

The Cloud

In the past, the storage and processing of electronic data chiefly took place at fund groups (i.e., onsite). Recent years have witnessed increased use of cloud computing technology, through which the storage (and often the processing) of electronic information may be "outsourced" to offsite data centers, typically owned and operated by outside vendors (see inset at right). These vendors may also provide other services, such as software applications, operating systems, user authentication, encryption, and software maintenance.[14] Generally speaking, cloud service providers control the underlying infrastructure and, to varying degrees, cede control of other services to the customers (see inset below).

Choosing a Cloud: Private, Community, Public, or Hybrid

The National Institute of Standards and Technology has published definitions of cloud computing and described the key deployment models as follows:

- ***Private Cloud*** – The cloud infrastructure is established for a specific organization, and access to it is limited to that organization. The infrastructure may be owned, operated, and managed by the organization and/or a third party, and the cloud exists on or off the premises of the sponsoring organization.
- ***Community Cloud*** – The cloud infrastructure is used by organizations with shared concerns. The infrastructure may be owned, operated, and managed by one or more of the sponsoring organizations and/or a third party, and the cloud exists on or off the premises of one or more of the sponsoring organizations.
- ***Public Cloud*** – The cloud infrastructure is established for public use, and access to it is generally limited to subscribers. The infrastructure is owned, operated, and managed by a sponsoring organization, and the cloud exists on the premises of the cloud provider.
- ***Hybrid Cloud*** – This is a combination of two or more types of clouds.

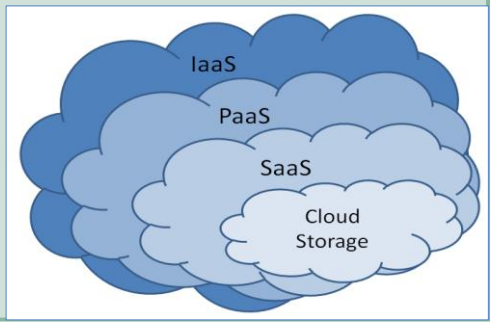
See Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145, National Institute of Standards and Technology, Information Technology Laboratory, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Sept. 2011).

Cloud storage can offer significant benefits to organizations, including ready access to data, competitive storage and maintenance costs, strong physical and electronic security at cloud data centers, optional encryption, and offsite backups. Other cloud computing services also offer potential benefits analogous to those provided by cloud storage, including relatively low costs for significant computational power, ready access to information and software, and the shifting of infrastructure development and maintenance costs to third parties.

Beyond Cloud Storage

Examples of different levels of cloud services beyond storage include the following:

- ***Software as a Service (or "SaaS"):*** In this arrangement, a customer is limited to the use of software applications provided by the cloud service provider.
- ***Platform as a Service (or "PaaS"):*** In this arrangement, a customer provides its own software applications that will be run on the infrastructure provided by the cloud service provider.
- ***Infrastructure as a Service (or "IaaS"):*** In this arrangement, a customer has the greatest level of control, including control over the storage, operating systems, applications, user authentication, encryption, and software maintenance.



[14] *See* The NIST Definition of Cloud Computing, Special Publication 800-145, Nat'l Inst. of Standards and Tech., Info. Tech. Lab., Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Notwithstanding its benefits, cloud computing present a number of additional challenges for fund groups (particularly with respect to the protection of data). Key risks associated with cloud computing include:

- ***Security of Third-Party Service Providers:*** Fund groups are understandably reluctant to relinquish control of data storage and processing to a third-party service provider. In deciding whether to use cloud storage and/or computing, fund groups may wish to consider, in particular, the level of physical and electronic security of the cloud provider's facilities.[15]

- ***Reliability:*** Fund groups should also consider the reliability of cloud service providers, as even the most robust cloud service providers have experienced some down-time.[16] Moreover, as cloud storage and computing depend on Internet access, fund groups should also consider the reliability of their Internet service providers.

- ***Regulatory Compliance:*** The use of cloud computing by fund groups may present challenges with respect to regulatory compliance. For example, fund groups may wish to consider how to ensure compliance with recordkeeping obligations in the event that a cloud service provider fails to safeguard information, and also to consider whether the use of cloud service providers (who may be domiciled in, or store information in, other states or even countries) has implications for compliance with privacy laws.

- ***Employee Use of Cloud Storage:*** *Employees'* own use of cloud storage may also present risks, including the potential for transmitting an organization's sensitive information to the employees' personal cloud storage accounts. Moreover, once information has been stored in personal cloud storage accounts, employees may more readily access such information through devices that lack firm-required security software (e.g., personal laptops and tablets).

Fund groups typically take a variety of steps to address these risks. To address reliability concerns, some fund groups have established more redundancy in their data storage. For example, one fund group downloads data from the in-house retirement plan provider's website and maintains the records (in encrypted form) on local servers. Fund groups may also pay particular attention to contractual provisions relating to computer security compliance by third-party service providers. A more complete discussion of compliance and risk management approaches relevant to cloud computing begins on page 13.

---

[15] Jackie Noblett, *Security, Control Concerns Cast Shadow on Cloud Adoption*, Ignites, June 6, 2012, http://www.ignites.com/c/365642/41522/Security_Control_Concerns_Cast_Shadow_on_Cloud_Adoption?referrer_module=searchResults&module_order=3&highlight=security+control+concerns; Jackie Noblett, *Is a Tech Failure the Next 'Black Swan' Event?*, Ignites, Feb. 16, 2012, http://www.ignites.com/c/314552/36492/Is_a_Tech_Failure_the_Next_Black_Swan_Event?referrer_module=searchResults&module_order=2&highlight=tech+failure+the+next.

[16] *See e.g.*, Claire Cain Miller, *Amazon Cloud Failure Takes Down Web Sites*, The New York Times, April 21, 2011, http://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/.

Compliance and Risk Management

Previous ICI Mutual studies have described some of the approaches taken by fund groups for protecting computer networks and the information accessed and stored on those networks. Recognizing that no single technique or set of techniques may be fully effective in preventing computer security incidents, fund groups tend to rely on a **layered approach to computer security**.[17] In broad outline, the approaches described in ICI Mutual's earlier studies (see inset) have not changed significantly with the emergence of mobile computing and cloud computing, but fund groups have modified and refined their approaches to computer-based risks over time in response to these and other evolving technology-based risks.

Computer Security Programs

Effective computer security programs tend to focus on three key goals:

- ***Prevention of security incidents*** – Effective computer security programs rely on various defensive techniques to prevent computer security incidents. These techniques focus on (1) blocking avenues for illicit access and use of computer networks, (2) ensuring that access and use is limited to users who are authorized to use the computer networks and whose identities have been authenticated, and (3) devising mechanisms to monitor, audit, and test the computer security defenses in place.
- ***Detection of incidents or attempted incidents*** – Effective computer security programs seek to detect, in a timely fashion, any incidents that do occur, along with their source, scope, and objective. Early intrusion detection may help prevent significant damage from occurring and permit fund groups to better safeguard uncompromised systems and data.
- ***Mitigation of harm*** – Effective computer security programs seek to limit damage and disruption from computer security incidents, restore normal business operations as promptly as possible, and seek recovery for losses from other parties where appropriate.

In developing risk management programs to address computer security issues generally (as well as concerns arising from mobile and/or cloud computing specifically), fund groups tend to consider some or all of the following topics and approaches: (1) **authentication and authorization**; (2) **protection of mobile devices**; (3) **encryption**; (4) **contractual protections**; and (5) **employee training and education**.[18]

AUTHENTICATION AND AUTHORIZATION

Authentication describes the process of confirming the identity of a user who seeks access to protected computer networks, and authorization encompasses the degree of access a duly authenticated user is permitted with respect to such networks. Many fund groups require a more stringent authentication process for remote users (e.g., hardware tokens, biometric identification, or other type of two-factor authentication).

Particularly given the potential vulnerabilities associated with mobile technology, fund groups may also wish to consider whether employees and other insiders should be permitted the same level of access when they are using remote access (and likely to be using wireless connections), as when they are accessing network resources via wired connections from their offices. Having tiered levels of remote access allows an organization to limit the risk it incurs, through permitting

---

[17] *See, e.g.*, Jackie Noblett, *What Funds Are Doing to Fend Off Hackers, Data Leaks*, Ignites, June 3, 2011, http://www.ignites.com/c/204042/25792/What_Funds_Are_Doing_to_Fend_Off_Hackers_Data_Leaks?referrer_module=searchResults&module_order=1&highlight=fend+off+hackers.

[18] The Federal Communications Commission's online cyber planner is an additional resource designed to help businesses develop customized cybersecurity plans. *See* Cyber Security Planning Guide, Fed. Commc'ns Comm'n (undated), *available at* http://transition.fcc.gov/cyber/cyberplanner.pdf.

the most-controlled devices (e.g., wired desktop computers) to have the most access and the least-controlled devices (e.g., personal mobile devices) to have the least access.

PROTECTION OF MOBILE DEVICES

The increasing use of mobile devices by employees and service providers has fostered debates over the extent to which sensitive information should be stored on such devices. Here, there is a natural tension between convenience and security. While some fund groups seek to eliminate the storage of any sensitive information on mobile devices (such that they are simply "portals" into the fund groups' computer networks), others have taken a different approach in which they seek to minimize the storage of information, but recognize that under certain circumstances (e.g., in the absence of Internet access), users may be unable to work effectively without having information stored on mobile devices.[19]

Where mobile devices are owned by fund groups, and where storage of sensitive information on such devices is permitted, fund groups typically take steps to safeguard such information in the event of the loss, theft, misplacement, or replacement of the devices. Thus, separate and apart from limiting access to sensitive information in the first instance, fund groups may take steps to configure the devices to erase all data if a user enters an incorrect password more than a given number of times. Many fund groups may also retain the ability to remotely lock and even "wipe" (i.e., erase data saved on) mobile devices in the event of loss, theft or misplacement. In addition, some groups may seek to limit the ability to print documents from mobile devices because of potential difficulties in protecting information once it has been printed at an offsite location.

User-owned devices, by contrast, may be more difficult for fund groups to protect. To the extent that fund groups permit the dual use of employee-owned devices (see discussion on page 18), they may wish to consider how to ensure that sensitive information is protected and timely removed from such devices. Some organizations utilize mobile device management software that can, among other things, restrict the use of mobile devices, track their location, audit their use, and set and enforce password policies. Some organizations also implement policies governing how employees may replace devices that are used for both personal and corporate use.[20]

ENCRYPTION

Encryption refers to the process of encoding data so that it cannot be read or understood without entry of a user password or other means of deciphering the data. The use of encryption by fund groups can depend on the context and the type of data, with certain categories of data—notably, data transmitted in online transactions—routinely encrypted. Other categories of data—including shareholder information, information in offsite backup or storage, internal corporate information (which may include information about employees), and information shared with contractors and/or service providers—may or may not be routinely encrypted, although use of encryption appears to be increasing.

---

[19] Even where information is not stored on mobile devices, there may be concerns regarding remote access. Indeed, one fund group reports that some of its private advisory clients seek to prohibit or severely restrict such access.

[20] *See, e.g.*, Michael A. Davis, *One Mobile Device Security Threat You Haven't Considered*, Oct. 5, 2011, http://www.informationweek.com/security/mobile/one-mobile-device-security-threat-you-ha/231900088.

Three factors appear to be contributing to the increased use of encryption. First, under many state privacy laws (see inset below), encryption may relieve companies of the obligation to provide notifications to customers in the event of a data breach. Second, given the increased popularity of mobile devices with their attendant risks (chiefly, loss, theft or misplacement), and given that it may be difficult or impractical to remove *all* information from such devices, some fund groups seek to further reduce these risks by requiring the encryption of information stored on mobile devices used by employees. Third, use by fund groups of cloud storage and cloud services can provide additional impetus for the use of encryption, since information may be stored on "outsourced" servers that are not under a fund group's direct control.

In evaluating whether, and to what extent, to encrypt information, fund groups may wish to consider a number of factors, including, among others: the degree to which any increased protection outweighs any loss of functionality or convenience for the users; the potential risk that encrypted information may not be accessible if passwords are lost or temporarily unavailable; and the scope of contractual protections that may be available from cloud service providers for loss or breach of data entrusted to them.

Evolving State of Data Security and Privacy Laws

Fund groups should be sensitive to applicable laws and regulations relating to data security and/or privacy. While a full discussion of these laws and regulations is beyond the scope of this study, a few points bear mention:

- ***State:*** Under laws in effect in most states, companies are required to notify customers in the event of a data breach. Typically, data breach notification laws provide for a number of exceptions to the notification requirement; of particular relevance for fund groups is the common exception for breaches involving encrypted information.
- ***Federal:*** Fund groups should consider federal securities laws and regulations. For example, funds and their advisers have long been subject to Regulation S-P, which relates to the privacy of consumer financial information. In October 2011, the SEC's Division of Corporation Finance released guidance to companies regarding disclosure obligations relating to cybersecurity risks and cyber incidents. To date, the SEC staff's guidance is directed only at certain public companies (not including investment companies).
- ***International:*** As many fund groups have expanded their operations across the globe, they may be subject to various international privacy laws, at least some of which can be more stringent than analogous U.S. laws. European data privacy laws, for example, are in many respects among the most stringent in the world, with potentially severe penalties.

See CF Disclosure Guidance: Topic No. 2 (Cybersecurity), Div. of Corp. Fin., SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

CONTRACTUAL PROTECTIONS

Today, many fund groups take into account various cyber risks when entering into or renewing contracts with their service providers. The emergence of cloud computing, in particular, has highlighted the importance to fund groups of evaluating the nature and scope of contractual protections. Indeed, at least one fund group has found it useful to revisit *all* of its contracts and to consider whether any of those contracts should be updated or renegotiated in light of technology issues. The contract negotiation process can serve a twofold purpose: first, to assist fund groups in reducing the possibility of cybersecurity incidents occurring in the future, and second, to clarify (and in some cases, to shift) the burden of any losses that may result from such incidents.

In seeking to reduce the possibility of cybersecurity incidents occurring in the future, some fund groups use the contract negotiation process as an opportunity to assess the data protection programs utilized by their third-party service

providers and business partners, particularly where sensitive information is involved. Recent SEC guidance emphasizes the importance of conducting such assessments.[21] ISO/IEC 27001 certification and SSAE 16 (formerly SAS 70) are commonly used auditing standards for assessing security compliance.[22] It should be noted that audit standards may vary (i.e., have different scopes and limitations) and may accordingly provide different levels of assurance to fund groups relying on them. In appropriate cases, fund groups may also wish to consider whether their providers and partners have EU Safe Harbor certifications (indicating compliance with the generally more stringent European data protection requirements).[23]

Contract negotiations may also enable fund groups to bind service providers and business partners to undertake certain actions designed to reduce the possibility of future cybersecurity incidents. For example, non-disclosure agreements between fund groups and their service providers (or other business partners) might be structured to require adherence to preset compliance procedures regarding the protection of sensitive information.

In clarifying the burden of any losses that may result from cybersecurity incidents, a number of fund groups emphasize the importance of focusing on indemnification issues in contracts with their service providers (and other business partners). In many cases, service providers may seek to limit their liability to a set amount (frequently, to the level of fees paid by the fund group). Given that potential losses may greatly exceed the level of fees paid, however, such limitations may expose fund groups to significant potential liability (for which insurance may be unavailable). A general discussion of liability (and insurance) issues associated with outsourcing of specialized functions by investment advisers and their affiliates can be found in a 2008 ICI Mutual risk management study, entitled *Outsourcing by Advisers and Affiliated Service Providers*.

EMPLOYEE TRAINING AND EDUCATION

The "human factor" is viewed by many experts as the weakest link in any cyber risk management program. Many cybersecurity incidents may be traced to employees, whether by error, carelessness, or design.[24] While cybersecurity incidents may in some cases be traced to intentional misconduct by employees, their inadvertent actions arguably present

---

[21] *See CF Disclosure Guidance: Topic No. 2 (Cybersecurity),* Div. of Corp. Fin., SEC (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[22] For information on ISO/IEC 27001 and SSAE 16, *see* www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103; http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf. Some practitioners advising on the use of ISO/IEC 27001 certification suggest making sure that the provider is *currently* certified, and note that the mere fact of certification does not necessarily indicate the quality of the security provider's controls. Other standards include the Cloud Security Alliance Cloud Controls Matrix. For a discussion of cloud security principles and for information on assessing the security of cloud providers, *see* https://cloudsecurityalliance.org/research/ccm/.

[23] For an overview of the European Union's approach to data protection, *see* Protection of Personal Data, European Commission, http://ec.europa.eu/justice/data-protection/index_en.htm.

[24] *See* The Insider Threat to U.S. Government Information Systems, Nat'l Sec. Telecommunc'n and Info. Systems Sec. Comm. (July 1999), at http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf (categorizing potentially harmful insiders into four categories, ranging from "traitor" to "well-intentioned"). *See also* Ellen Messmer, *Young Employees say BYOD a 'right' not 'privilege'*, Network World, June 19, 2012, http://www.networkworld.com/news/2012/061912-byod-20somethings-260305.html (finding that two-thirds of employees have violated or would violate restrictions on using personal devices for work purposes).

a greater threat to organizations. As a result, even the most comprehensive policies, backed by the latest technology, may prove inadequate to ensure strong cybersecurity.

In recognition of the "human side" of the risk equation, many groups have taken steps to raise employee awareness. Thus, for example, employee manuals typically include specific policies on data security, and in some fund groups, employees may be required to certify on a periodic basis that they understand and agree to these policies. Written policies may have their inherent limitations, however. In this regard, while more comprehensive policies may provide employees with more specific guidance on addressing data security issues, they may prove to be too complex or dry to serve as a ready reference for employees. Conversely, while policies that are more principle-based may be more accessible, they may provide inadequate guidance for specific situations. Moreover, written policies, particularly those that are more comprehensive and detailed, may quickly become outdated.

To address inherent shortcomings of written policies, fund groups have sought to supplement them in a variety of ways. Some groups, for example, send periodic news alerts or bulletins to employees about specific data security issues and initiatives. Such bulletins may include, for example, reminders to employees to use recycling bins, to lock filing cabinets that contain sensitive information, not to use personal cloud storage accounts, or not to leave passwords in plain sight, and/or may focus on current news events pertaining to data security. One fund groups reports introducing a "personal shred day" on which employees are encouraged to bring personal documents to the office for destruction. Another group has a "clean desk" policy under which employees receive warnings if they leave sensitive information on their desks overnight.

Some fund groups highlight the importance of promoting a broader cultural emphasis on data protection. As one employee interviewed for this study noted, even a brief discussion by a CEO of confidentiality and privacy concerns at a monthly meeting can be helpful in raising employee awareness and sending the message that data security is a priority at all levels of the organization.[25]

[25] *See also* Dominic Saunders, InsuranceTech, *4 Reasons Security Policies Fail, And 7 Steps to Make Sure They Don't*, Sept. 11, 2012, http://www.insurancetech.com/security/240006849.

The Dual-Use Dilemma: The "Bring Your Own Device" (BYOD) Trend

The use of personal (i.e., employee-owned) mobile devices for business purposes (e.g., accessing proprietary company resources such as email, file servers, and databases) epitomizes the challenges faced by fund groups (and other employers) in addressing a rapidly changing technological landscape. As personal mobile devices are used increasingly in the workplace, fund groups may find it challenging to balance their employees' interests in using a single, powerful device for both business and unrestricted personal use against their IT and compliance departments' interests in developing and maintaining robust security protections and procedures.

If employees are allowed to use their own mobile devices for work-related functions, fund groups may wish to consider adopting formal BYOD policies that clearly outlines the groups' expectations and requirements relative to, among other things, employee privacy, data confidentiality, and device management and support. While the design and implementation of BYOD policies can vary significantly, such policies often address the following areas, among others:

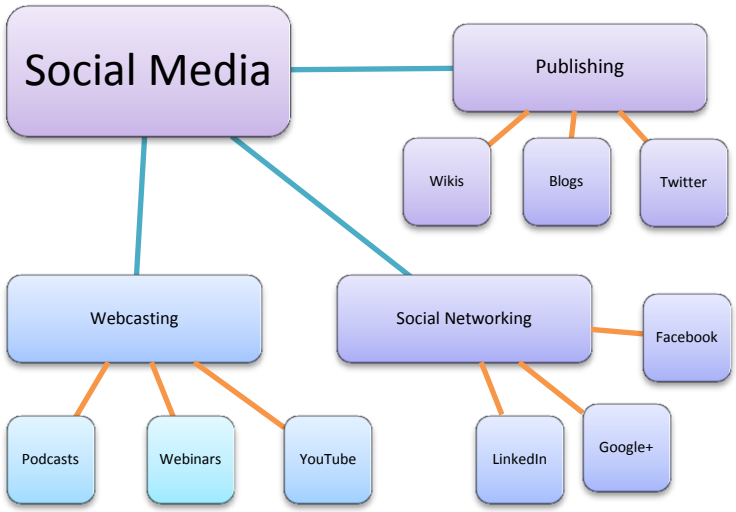
- ***Security measures on devices*** – Some organizations require personal devices to be configured with passwords, prohibit specific types of applications from being installed on the devices, require the segregation of personal and corporate information stored on devices (e.g., through use of mobile device management software), and/or mandate that all data on the devices be encrypted.
- ***Network access restrictions*** – Some organizations restrict activities that employees are allowed to perform on BYOD devices (e.g., email usage is limited to corporate email only) and/or preclude access to certain types of data (e.g., shareholder account information). Organizations may bar certain employees or groups of employees (e.g., human resources personnel) from using BYOD devices, given the nature of their job responsibilities.
- ***Corporate control over devices*** -- Some organizations may require that employees using BYOD devices agree to some level of corporate control. Thus, for example, employees may be required to agree, in writing, that if their devices are lost or stolen, or if they enter an invalid password in excess of a given number of times, all information on the devices (some of which may be personal) may be "wiped" remotely through the company's mobile device management system. Because corporate control over such devices may give companies the ability to access personal information, the BYOD trend may also create potential new challenges with respect to employee privacy.
- ***Maintenance of security measures*** – The BYOD policies of some organizations may assign responsibility for maintaining security protections (such as keeping anti-virus software up-to-date) to the mobile device owners (i.e., employees) instead of to the organizations' own IT departments. In such cases, IT departments may be responsible for troubleshooting only certain types of problems on employee-owned devices (e.g., problems associated with corporate software, and not problems associated with the devices' operating systems).
- ***Auditing of device security*** – The BYOD policies of some organizations may provide for periodic IT audits to ensure that each personal mobile device is in compliance with applicable BYOD policies.

Social Media: Protecting Reputation and Ensuring Regulatory Compliance

As the nature of communications on the Internet has evolved, the so-called "social media" have assumed greater prominence and significance. Simply stated, the rise of social media has resulted in a shift from unilateral monologues by organizations (e.g., via their websites), towards bilateral and multilateral "conversations" between and among organizations, their customers, their business partners, and the general public, via the Internet. This section provides a general introduction to social media, to the key risks to fund groups associated with their use, and to approaches that may assist fund groups in managing these risks.

Social Media

The term "**social media**," as used in this study, refers to Internet-based services or applications that permit fund groups to interact with their shareholders or potential shareholders, service providers, or other communities of users. The most relevant types of social media for fund groups include: (1) **social networking** (i.e., expanding contacts and connections, for example, through Facebook, Google+, or LinkedIn); (2) **publishing** (i.e., distributing written materials through wikis, blogs and microblogs, including Twitter); and (3) "**webcasting**" (i.e., disseminating audio or video materials, for example, through YouTube videos, or by means of podcasts or webinars).[26]



Some fund groups are actively using social media,[27] while others are still weighing their

[26] *See* Mariana Lemann, *How Different Firms Use Social Media*, Ignites, July 26, 2012, http://www.ignites.com/c/387862/43962/How_Different_Firms_Use_Social_Media?referrer_module=searchResults&module_order=36&highlight=social+media; Peter Ortiz and Danielle Sottosanti, *Firms Focus Social Media Strategy*, Ignites, March 14, 2012, http://www.ignites.com/c/326802/37722/Firms_Focus_Social_Media_Strategy?referrer_module=searchResults&module_order=24&highlight=firms+focus+social+media.

[27] Investment advisers (both fund and non-fund) have adopted social media strategies. *See, e.g.*, Jackie Noblett, *Mobile Drives Advisor Adoption of Social Media: Study*, Ignites, Apr. 18, 2012, http://www.ignites.com/c/342172/39272?highlight=mobile%20drives%20social%20media (noting that advisers are using social media more often for business purposes).

associated costs and benefits.[28] Fund groups who have opted to use social media cite a variety of reasons for doing so, including:

- ***Ease and speed of communications:*** Social media lend themselves to timely and relevant communications. The relative informality of social media may be a factor permitting faster—and less expensive—communications. The ease with which users may share information has also been cited as an advantage.[29]

- ***Internal consumption of content:*** Some fund groups have found social media helpful in disseminating content within their organizations (e.g., to employees and business partners), through the use of private groups, intranet sites, and wikis.

- ***Fear of missing out (or FOMO):*** Given the rapid adoption of social media by the public, some companies have expressed concern that a failure to adopt social media could leave them at a competitive disadvantage.

Generally speaking, the information transmitted by means of social media tends to be "public," in the sense that it is not confidential or otherwise sensitive. As a result, the key risks presented by social media for fund groups tend to be regulatory and/or reputational risks (although these risks, in turn, may ultimately result in financial damage). The rise of social media presents regulatory challenges for fund groups, as they grapple with new regulatory compliance issues (or new takes on old ones). Moreover, the online "conversations" fostered by social media, combined with the speed of their communication, create the opportunity for corporate reputations built over decades to be sullied in a short period of time.

REGULATORY RISK

In recent years, regulators have begun to focus particular attention on the use of social media by fund groups and other financial institutions. However, the regulatory guidance issued to date, and the industry's mixed reactions to the guidance, suggest that it may take years to reconcile regulatory requirements with the growth and prevalence of social media. In the meantime, fund groups will continue to face challenges in working within the existing regulatory framework.

[28] Some companies have, to date, refrained from adopting social media strategies due, in part, to skepticism about the benefits of doing so. Even assuming that the use of social media will yield benefits, some fund groups have expressed concern about how to measure the return on investments in social media, particularly given the difficulty of quantifying some of the benefits.

[29] One fund group has suggested, for example, that given consumer expectations regarding the necessary level of production values, a YouTube video could be produced at a fraction of the time and cost of a more traditional video presentation.

Social media communications may implicate various federal securities laws and regulations,[30] including the following:

- ***Recordkeeping requirements:*** Social media communications can be subject to recordkeeping obligations under the federal securities laws.[31] Firms using social media need to make sure that they are able to capture and retain all required information.

- ***Advertising restrictions:*** Federal securities laws and regulations impose restrictions on advertising by funds and advisers. These restrictions may apply to social media communications in certain circumstances (i.e., where communications relating to specific funds or products might be construed as advertising).[32]

- ***Prohibition against testimonials:*** In some instances, social media postings by employees or third parties could be construed as testimonials for investment advisers, so as to be subject to applicable regulations.[33]

- ***Other laws and regulations:*** Social media communications may also implicate a range of other laws and regulations, including Regulation FD, antifraud provisions, data privacy, and proxy solicitation rules, among others. [34]

Fund groups have, over the years, generally developed appropriate policies and procedures to address regulatory requirements governing more traditional types of communications (e.g., written correspondence, oral statements, e-mails). At one level, social media communications may be viewed simply as variations on traditional forms of communication. However, the very speed and informality of social media communications, as well as the difficulties faced by fund groups in monitoring and controlling the multiple channels for such communications, set them apart. As a result, some fund groups have chosen to develop stand-alone social media policies to supplement their existing compliance and risk management efforts. A more complete discussion of compliance and risk management approaches relevant to social media begins on page 23.

---

[30] *See* Rajib Chanda and Anu Heda, *How Firms Navigate Social Media Regulatory Uncertainty*, Ignites, Mar. 9, 2012, http://www.ignites.com/c/325332/37522/How_Firms_Navigate_Social_Media_Regulatory_Uncertainty?; Peter Ortiz, *Mass. Probing Advisors' Use of Social Media,* Ignites, May 27, 2011, http://www.ignites.com/c/201792/25512/Mass_Probing_Advisors_Use_of_Social_Media?.

[31] *See*, *e.g.*, Advisers Act section 204 and rule 204-2 thereunder. *See also Investment Adviser Use of Social Media*, National Examination Risk Alert, SEC, Office of Compliance Inspections and Examination, Jan. 4, 2012, http://www.sec.gov/about/offices/ocie/riskalert-socialmedia.pdf.

[32] *See* James Hardaway, Jr., *How Should Funds Assess Social Media Risk/Reward?*, Ignites, Aug. 31, 2012, http://www.ignites.com/c/404041/45531/How_Should_Funds_Assess_Social_Media_RiskReward?.

[33] *See* rule 206(4)-1(a)(1). *See* Rajib Chanda, *How Do Fund Firms Regulate Social Media Testimonials,* Ignites, May 29, 2012, http://www.ignites.com/c/361262/41152/How_Do_Fund_Firms_Regulate_Social_Media_Testimonials?.

[34] *See In Netflix Case, a Chance to Re-examine Old Rules*, New York Times (Dec. 11, 2012), http://dealbook.nytimes.com/2012/12/11/in-netflix-case-a-chance-for-the-s-e-c-to-re-examine-old-regulation/.

In early January 2012, after surveying investment adviser use of social media, the SEC staff issued a National Examination Risk Alert. The staff set forth factors (see inset) for advisers to consider in constructing their social media policies, and emphasized the need to comply with various provisions of the federal securities laws, including their antifraud, compliance, and recordkeeping provisions.

Social Media Policies: SEC Factors to Consider

In its National Examination Risk Alert, the SEC staff set forth a lengthy, but "non-exhaustive," list of factors for advisers to consider in constructing social media policies, including:

- Usage guidelines on the appropriate use of social media
- Content standards, restrictions, and approval
- Means and frequency of monitoring adviser's own social media site and third-party sites
- Level of resources dedicated to social media monitoring
- Criteria for approving participation in social media site
- Training requirements of appropriate personnel
- Certification of compliance with social media policies and procedures
- Information security risks

See Investment Adviser Use of Social Media, National Examination Risk Alert, SEC, Office of Compliance Inspections and Examination, Jan. 4, 2012, http://www.sec.gov/about/offices/ocie/riskalert-socialmedia.pdf.

In providing guidance on the use of social media, the Financial Regulatory Authority (FINRA) has issued various regulatory notices and has itself used social media, such as podcasts and webinars, to disseminate relevant information. Over the past few years, FINRA has provided guidance on firms' compliance obligations with respect to the use of social media websites for business communications to the public, and has also implemented some changes to its rules regulating such communications.[35]

REPUTATIONAL RISK

Communications on social media—and, more broadly, on the Internet—may present reputational risk to fund groups. Fund groups, along with other financial institutions, may be subject to a variety of threats (from insiders as well as outsiders), including "dummy" websites (i.e., unauthorized websites, purporting to be those of the fund groups themselves, which may be used to improperly gather information from unsuspecting fund shareholders or potential fund shareholders), "wiki attacks" (i.e., where wiki users highlight negative publicity on a firm's page), improper testimonials, false affiliations, false endorsements, trademark infringement, the improper use of proprietary information, or, simply, flat-out damaging statements. In one instance, for example, fraudsters created a fake Google+ presence for a financial institution.[36] In another, a fraudulent website warned against doing business with certain affiliates of an investment adviser.

To mitigate reputational risk, some fund groups emphasize the need to monitor their presence on the Internet and in social media (see discussion beginning on page 24). For these groups, the costs of such monitoring are outweighed by the

---

[35] *See, e.g.*, *Communications with the Public*, FINRA, Regulatory Notice 12-29 (June 2012), http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p127014.pdf; *Social Media Websites and the Use of Personal Devices for Business Communications*, FINRA, Regulatory Notice 11-39 (Aug. 2011), http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p124186.pdf; *Social Media Web Sites*, FINRA, Regulatory Notice 10-06 (Jan. 2010), http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf.

[36] Julia La Roche, *Bank Of America Just Had The Ultimate Social Media Fail*, Business Insider, Nov. 15, 2011, http://www.businessinsider.com/bank-of-america-google-plus-page-2011-11?utm_source=feedburner.

potential reputational costs. For many, the speed of social media communications requires an equally rapid response. As one observer has noted, "Companies need to act at warp speed." A quick response in turn requires early detection of potential issues.

Compliance and Risk Management

In developing risk management programs to address the regulatory and reputational risks presented by social media, fund groups tend to consider the following three areas: (1) how a fund group itself will be using social media (if at all); (2) how a fund group is portrayed by others in social media (and, more broadly, on the Internet); and (3) how a fund group's employees' use of social media affects the fund group.

FUND GROUP USE OF SOCIAL MEDIA

Fund groups may find it helpful to establish specific social media policies to set forth how they will be using social media and ensuring regulatory compliance.[37] It is worth noting that even fund groups not directly engaged in social media may find it helpful or necessary to establish social media policies, as the fund groups may be affected by social media use by third parties and/or employees (as discussed in the following sections).

In establishing social media policies, fund groups seek to balance speed-to-market of social media communications against compliance considerations. In that regard, it may not always be clear which communications should be subject to prior approval by compliance personnel. For example, blog posts that could be construed as advertising may require enhanced scrutiny, while other blog posts may require no special review.[38]

Fund groups may wish to consider the extent to which they will permit third parties to post on the groups' own social media sites (e.g., on their Facebook pages). The SEC staff has expressed concerns about this practice. Fund groups are taking a variety of approaches to this issue. Some firms "allow third parties to post messages, forward links, and post articles" on social media sites, whereas some firms permit only "one-way postings" (i.e., the firm or its representative may

---

[37] Peter Ortiz, *Social Media Catches Eye of Compliance Pros: Survey*, Ignites, July 25, 2012, http://www.ignites.com/c/387992/43882/Social_Media_Catches_Eye_of_Compliance_Pros_Survey? , citing a survey by Lynne M. Carreiro and Karth D. Ireland, The Investment Adviser Association, ACA Compliance Group, IM Insight, and Old Mutual Asset Management, June 14, 2012, https://www.investmentadviser.org/eweb/Dynamicpage.aspx?webcode=DocRedirect&wps_key=6c736af4-4403-4576-b0f5- (fund testing for compliance with regulations pertaining to social media is on the rise with 52% of respondents replying that testing for compliance with social medial policies has increased since 2010); Lynne M. Carreiro, *How Can Firms Ensure Social Media Compliance?*, Ignites, July 15, 2011, http://www.ignites.com/c/221732/27542/How_Can_Firms_Ensure_Social_Media_Compliance?referrer_module=searchResults&module_order=189&highlight=social+media.

[38] *See* Davis D. Janowski, *FINRA, SEC Rules Constrain Advisers in Blogosphere*, InvestmentNews (Oct. 21, 2008), http://www.investmentnews.com/apps/pbcs.dll/article?AID=2008309019978, ("Because of disclosure and anti-fraud considerations, the information that advisers disclose on blogs requires the same compliance scrutiny as corporate press releases.")

post, but may not interact with third parties). Other firms are even more restrictive and prohibit postings by the general public.[39]

Some observers have emphasized the need for a social media strategy to have the participation and approval of all the major stakeholders in a fund group, including IT personnel, legal, compliance, marketing, and senior management. Perhaps in light of the relative novelty of social media and the difficulty in quantifying their benefits, some fund groups have encountered internal resistance to developing social media policies. Where social media policies have been adopted, some fund groups suggest the need to revisit those policies on a periodic basis and to stay abreast of new or changing risks associated with social media.[40]

EXTERNAL USE OF SOCIAL MEDIA AND THE INTERNET

As noted above, many groups emphasize the need to monitor social media and the Internet for potential threats (e.g., dummy websites).[41] Fund groups that perform such monitoring typically rely on a wide range of tools. These tools may include the relatively crude tool of creating "Google alerts" (i.e., automatic e-mail notifications of new content relevant to a given search), or conducting random Internet searches for references to fund groups. Fund groups may also rely, in part, on notifications, complaints, or alerts from shareholders or from third parties. Some fund groups have found it helpful to engage the services of third-party vendors that may, among other things, employ proprietary "web crawlers" (i.e., programs designed to collect information from the Internet at regular intervals) to find information relating to their organizations. Fund groups may also work directly with domain registry services to find and identify new or existing websites that have the potential to infringe upon a fund group's brand.

Once potential problems are identified, fund groups may find that there are various avenues to consider for resolving them. For example, in the case of fraudulent websites, fund groups may work with domain name registrars (e.g., Network Solutions) to have the sites taken down. In some cases, fund groups may be able to have such sites removed easily; however, in other cases, fund groups may need to resort to uniform dispute resolution procedures (or UDRP) to unmask the identity of the fraudsters, file complaints, and have the claims decided by arbitrators.

Fund groups engaged in the monitoring of social media and the Internet cite the difficulty of staying abreast of changing approaches by fraudsters, identity thieves, or other bad actors bent on causing harm or malicious mischief. For example, the ability to purchase website domain names in Cyrillic or in Chinese characters provides new opportunities for fraud. The proposed plan by the Internet Corporation for Assigned Names and Numbers ("ICANN") to permit new types of domain names (e.g., instead of ".com" or ".org", a domain may incorporate the company name, as in ".icimutual") raises similar issues. Some fund groups are concerned that these and other developments could require them to spend

---

[39] *See Investment Adviser Use of Social Media, National Examination Risk Alert*, SEC, Office of Compliance Inspections and Examination, Jan. 4, 2012, http://www.sec.gov/about/offices/ocie/riskalert-socialmedia.pdf.

[40] *See* Andrew Greene, *LinkedIn Hack Pushes Firms to Rethink Social Media Policies*, Ignites, June 11, 2012, http://www.ignites.com/c/367312/41722/LinkedIn_Hack_Pushes_Firms_to_Rethink_Social_Media_Policies?.

[41] One fund group observed that an additional benefit of monitoring is to help protect shareholders by removing social media posts in which shareholders divulge personal information or account information.

significant amounts of time and money to protect their reputations and brands, and may make it easier for fraudsters to confuse customers about the legitimacy of sites. In the view of these fund groups, monitoring becomes increasingly important.

EMPLOYEE USE OF SOCIAL MEDIA

In monitoring social media and the Internet, companies may be well advised to specifically consider employee use.[42] Some experts warn of potential legal and reputational harm that may result from inadvertent or intentional misuse of social media by employees. For example, employee postings on social media may fall afoul of restrictions on advertising or on the use of testimonials. Moreover, social media postings may play a role in, among other things, creating a hostile work environment, fostering discrimination, defaming other employees or outsiders, or disclosing confidential information.

In seeking to limit the potential harm from employee use of social media, fund groups tend to rely on various defenses, which may include employee training, limitations on use by employees of social media in the workplace, and/or monitoring of social media activity by employees.

- ***Training:*** Many fund groups emphasize the need to focus on employee training about what can and cannot be done on social media. Some groups have issued broad guidance regarding social media and/or electronic communications generally, and have issued more specific advice, as needed, on social media topics. Effective training approaches also share many of the following features: clarification about what constitutes a business communication (including site-specific advice and device-specific advice); a mechanism for employees to ask questions; the establishment of a penalty structure; and a mechanism for periodic reviews of the training process. Given the rapid developments in social media, some fund groups have focused on how to more quickly impart up-to-date information to employees. At least one fund group sends regular bulletins to employees with the latest in IT news.

- ***Limitations on Use:*** Fund groups have also considered whether to impose limitations on the use of social media by employees. Some fund groups have sought to ban the use of social media in the workplace or to confine Internet access to trusted sites, even as they recognize that employees may have ready access to social media sites or the Internet on their personal mobile devices. Others have a more targeted approach, under which employees are generally banned from posting as part of their *professional* responsibilities, absent prior approval or review of postings.

- ***Monitoring of Employee Activity:*** Monitoring social media activity of employees may be a daunting task, particularly at large fund groups. Effective monitoring requires a thorough and efficient review of potentially

[42] James Needham, *How Fund Firms Can Monitor Social Media*, Ignites, Aug. 3, 2012, http://www.ignites.com/c/392362/44312/How_Fund_Firms_Can_Monitor_Social_Media_?.

voluminous social media postings.[43] Some funds actively monitor all or some social media activity that take place on their computer networks. In determining the scope of monitoring, fund groups may wish to consider whether particular types of social media require closer scrutiny than others. For example, LinkedIn is often viewed as the social networking site for business professionals, and, as a result, may be more prone to have business-related communications. A few fund groups seek to expand the scope of their monitoring to include social media activity that takes place outside the corporate networks (e.g., on employees' personal equipment). Outside the fund industry, some organizations are reportedly requiring employees to provide their passwords to social media sites in order to allow monitoring, but this form of monitoring does not appear to be common and may be prohibited in at least some states. Other organizations, including some fund groups, have engaged the services of third-party vendors to monitor social media use by employees.

It is important to note that monitoring and/or restricting employee use of social media (whether in the workplace or outside of the workplace) may raise other potential issues for fund groups relating to employee privacy rights, free speech protections and employment and labor practices.[44] In developing an effective social media policy for employees, fund groups must consider and balance a number of competing interests and legal requirements. Fund groups may find it prudent to consult with legal counsel in developing and implementing their social media policies, particularly where such policies are more restrictive.

---

[43] Lisa Vaas, *Employers On Track To Get More Nosey With Employees' Social Media Lives*, May 31, 2012, http://nakedsecurity.sophos.com/2012/05/31/employers-on-track-to-get-more-nosey-with-employees-social-media-lives/ (citing study by Gartner, *Gartner Says Monitoring Employee Behavior in Digital Environments is Rising*, http://www.gartner. com/it/page.jsp?id=2028215).

[44] Peter Ortiz, *Labor Rules Could Force Rewrite of Social Media Policy*, Ignites, June 18, 2012, http://www.ignites.com/c/370802/42102/Labor_Rules_Could_Force_Rewrite_of_Social_Media_Policy (noting the potential for social media policies to infringe upon employee rights).

Insurance Considerations

In considering how to manage cyber risks in general, and risks associated with mobile computing, cloud computing, and social media in particular, fund groups may wish to consider the role of insurance in their risk management programs. In this regard, fund groups may wish to evaluate the extent to which their existing insurance policies may provide protection for some of these risks, and/or to evaluate the relative costs and benefits associated with specialty cyberliability insurance coverage. By necessity, this section generalizes as to the insurance issues discussed. Of course, the terms and conditions of individual insurance policies themselves (including any special endorsements that may be added to standard policy forms during the course of the insurance underwriting process) will govern any coverage questions arising in a particular matter.

"Traditional" Insurance Policies

The development of many "traditional" types of insurance policies—including general liability and property policies—long predated the ascendancy of the digital age. As a result, these traditional policies typically were not designed to cover cyberliabilities (i.e., liabilities associated with computers, networks, electronic data, and the Internet). In recent years, many insurers have sought to clarify that such policies do not generally respond to cyber risks.[45]

Fidelity Bonds and D&O/E&O Insurance Policies

By contrast to the "traditional" policies described above, investment company blanket bonds ("Bonds") and, to a lesser extent, mutual fund directors and officers/errors and omissions liability insurance policies ("D&O/E&O Policies") may provide some limited cyber coverages, typically at little or no additional cost. Certain of these coverages may be provided in the standard forms of the Bonds and D&O/E&O Policies, whereas others may be provided as separate components (or "insuring agreements") to Bonds. The most common of these coverages are as follows:

- ***Certain Fidelity Losses:*** The "Fidelity" insuring agreements of Bonds may protect insureds against fidelity losses resulting from an employee's dishonest or fraudulent acts in use of an insured's computer systems (e.g., if an employee were to hack into a shareholder's account and transfer funds to his or her own account).

- ***Certain Negligence-Based Losses:*** D&O/E&O Policies may respond to damages that an insured is required to pay to third parties in claims resulting from the insured's negligence in addressing computer security issues associated with the insured's investment management business.

---

[45] S*ee*, *e.g.*, Christine Phan and Catherine Colinvaux, *The State of Cyberinsurance*, at 2, Insurance Law360 (Mar. 7, 2011), *available at* http://www.zelle.com/assets/attachments/The%20State%20Of%20Cyberinsurance%20-%20Insurance%20Law360.pdf (observing that many traditional insurance policies "expressly exclude coverage for typical cyberlosses").

- ***"Online Transactions" Coverage:*** Bonds (through separate "insuring agreements") may protect insureds against third-party fraud in "online" requests for redemptions and other designated transactions in fund shares that are requested via an insured's Internet site(s) or other online systems.

- ***"Computer Security" Coverage:*** Bonds (through separate "insuring agreements") may protect insureds against certain losses incurred as a result of hacker attacks or similar unauthorized access to the insureds' internal computer systems. However, such coverage, being "hacker-oriented," may not cover attacks committed by or in collusion with insiders or other authorized users (such as third-party service providers).

Regardless of the scope of the particular cyber coverages provided, it is important to recognize that Bonds and D&O/E&O policies are not, nor are they intended to be, comprehensive cyber insurance policies. Bonds and D&O/E&O policies would typically not, for example, provide coverage for various exposures that might be insurable under cyber insurance policies (e.g., business interruption expenses, costs associated with data breaches, or "greenmail" payments in response to extortion threats to safeguard computer systems).

Specialty Cyber Insurance Policies

In recent years, a number of insurance companies have begun to offer specialty cyber insurance policies. While the types of coverage offered—and the cost of such policies—can vary widely, these cyber insurance policies are generally designed to replace and/or supplement the narrower coverages that may be available in other types of underlying insurance policies (such as Bonds or D&O/E&O Policies). Typically, cyber insurance policies (generally issued on a stand-alone basis) typically offer both first-party ("cybercrime") and third-party ("cyberliability") protection. Thus, for example, these policies may provide coverage for some or all of the following:

- ***Business interruption/extra expense*** (e.g., an insured's expense and loss of income after a computer security incident and, in some cases, expenses associated with the interruption of businesses on which the insured is dependent);

- ***Media liability*** (i.e., losses resulting from defamation and invasion of privacy claims, as well as from copyright or intellectual property infringement);

- ***Vicarious liability*** (e.g., for breaches committed by an insured's key service providers that affect the insured or its clients);

- ***Identity theft costs*** (e.g., costs of data breach notifications to potentially affected clients and/or costs of credit monitoring services);

- ***Crisis management expenses*** (e.g., public relations costs in the wake of a data breach);

- ***Loss resulting from theft or misappropriation of confidential or proprietary information***, including trade secrets or customer information;

- ***Loss from physical damage or destruction of computer systems or data*** (e.g., costs of damage assessment and repair following a computer security incident); and

- ***Payment of extortion threats*** relating to computer systems, applications, or data, or to theft of proprietary information.

To date, these specialty cyber insurance policies do not appear to have been widely purchased by fund groups. In the past, some fund groups reportedly had concerns over the costs of such policies; the limited availability of high insurance limits; the more extensive underwriting that was involved; and the need for sharing sensitive security information with outsiders (i.e., its insurer and computer security consultant). Recent years have seen some changes in the cyber insurance market that have mitigated—but not eliminated—these original concerns. In this regard, some fund groups have reported that the cost of such policies has declined over the past decade, and that the underwriting of such policies has become less onerous for fund groups.[46]

As a relatively new product, cyber insurance presents challenges for insurers and insureds. Insurers, for their part, lack extensive historical claims data, adding complexity to the pricing of the product.[47] Insureds, for their part, may have difficulty assessing their level of risk, making it difficult to gauge whether cyber insurance is a compelling value proposition. The passage of time may help address these challenges.

---

[46] The experience of fund groups with cyber insurance appears to have mirrored the experience of the corporate world generally. For an overview of the cyber insurance market, *see The State of Cyberinsurance*, *supra* note 45.

[47] *See id.*, at 3 ("Unlike with traditional insurance, where decades of actuarial information is available to help price the insurance, everyone is relatively new to e-commerce."); Edwards Wildman Palmer LLP, *Insuring Against Cyber Risks: Congress and President Obama Weigh In*, Mar. 2012, http://www.edwardswildman.com/newsstand/detail.aspx?news=2812.

ICI Mutual | *the safest decision you can make*

Unequaled industry knowledge and expertise:
We help insureds identify and avoid risk at the front end. We stand behind them if problems occur.

A history of stability and financial strength:
Our coverage has been available and consistent since our inception. And by reinsuring our policies, we've deliberately and prudently spread our own risk.

The best claims payment reputation in the industry:
As our insureds who have faced trouble with commercial insurers will tell you, we're dedicated to paying appropriate claims rather than haggling over them.

Not just a partner, a *good* partner:
We were created to serve the mutual fund industry and only the mutual fund industry. We answer only to our insureds and their needs.

ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry's managed assets. As the mutual fund industry's captive insurance company, ICI Mutual is owned and operated by and for its insureds. ICI Mutual's services assist insureds with identifying and managing risk and defending regulatory enforcement proceedings and civil litigation.

ICI Mutual also serves as a primary source of industry information regarding mutual fund insurance coverage, claims, risk management issues, and litigation developments. Publications include an extensive library of risk management studies addressing such topics as corporate action processing, investment management compliance, computer security, defense cost management, identity theft, independent director litigation risk, prospectus liability risk, and ERISA liability, and operational risk in managing private accounts, among others, and the *Investment Management Litigation Notebook*, risk manager alerts, and the annual *Claims Trends* newsletter. Additional services include peer group profiles, coverage analyses, and assistance to insureds and their counsel in litigation defense.

ICIMutual
A Risk Retention Group

1401 H Street NW, Suite 1000
Washington, DC 20005

800.643.4246
info@icimutual.com

www.icimutual.com