Computer Security Lite

Half the Jargon of Regular Computer Security (A Guide for Management)

Originally Published in December 2003

Computer Security Lite

Introduction and Executive Summary

ICI Mutual Insurance Company, a Risk Retention Group ("ICI Mutual" or the "Company") has conducted this study on managing computer security risks ("Study"). Written specifically for senior management, and legal and compliance personnel, the Study is designed to facilitate communications with computer security experts, and to assist fund complexes in identifying specific types of computer security risks and in developing and implementing computer security risk management techniques.

Fund complexes rely on, and indeed could not operate without, computer-based technology for information collection, storage, and processing.[1] The increased sophistication of computer technology in recent years has enabled fund complexes to expand the scope and volume of their operations, to outsource greater portions of these operations to third-party providers,[2] and to respond to demands by employees, fund shareholders, and brokers for ever-greater levels of Internet-based access and services. These and other developments have left computer systems used by most fund complexes increasingly "open," with critical data routinely available to affiliates, business partners, shareholders, and other third parties.[3] As a result, maintaining information security has become critical to fund operations. Breaches of computer security, whether by insiders or third parties, may permit misappropriation, destruction, or alteration of sensitive information (or of systems for processing such information in an accurate and timely fashion) and may have significant short-term and long-term adverse effects on the complex's financial health and reputation.

To date, the fund industry appears to have largely escaped significant losses arising from breaches in computer security. Yet the ongoing risk to the industry cannot be discounted. Indeed, available statistics point to the significant — and

growing — computer security problem at U.S. corporations (including financial institutions) and government agencies generally.[4] While the fund industry has long been sensitive to protection of financial information and to privacy concerns,[5] recent incidents of computer security breaches at large, well-known companies have highlighted that even the most sophisticated businesses are not immune from such risks.[6]

The observations in the Study are derived from ICI Mutual's detailed interviews with selected fund complexes, from discussions with outside computer security consultants, and from ICI Mutual's examination of publicly available information on computer security losses and related issues. The Study is not intended to and does *not* recommend any single structure or set of "best practices" to address computer security risks. Given the diversity of the investment management industry, it is not advisable or practical to seek a "one size fits all" standard for behavior in this area. Instead, effective management of computer security risks will depend upon many factors particular to the complex, including complex size, the scope and nature of the complex's use of computer-based technology, the extent of a complex's reliance on affiliates and third-party service providers, and the complex's overall compliance philosophy. Moreover, a set of best practices, even if it were feasible to devise one, would rapidly become obsolete.

The Study is divided into two sections:

- **Overview** — The first section presents general observations on computer security risks for fund complexes, and sets forth a series of questions that insured complexes may wish to consider in assessing their computer security risk management efforts.

- **Elements of an Effective Computer Security Program** — While it is neither realistic nor appropriate to expect fund complexes to adopt identical programs to manage computer security risks, there are certain themes and elements that are likely to be common to effective computer security programs. The second section describes these common themes and elements, and discusses questions that fund complexes may wish to consider in structuring their own computer security risk management programs.

Overview of Computer Security Risks

A computer security program, at its essence, is designed to protect identified categories of sensitive information — and systems and applications for collecting, storing and processing such information — from various types of cyber-based threats. In the fund industry, sensitive information can be broadly categorized to include: (1) shareholder information (e.g., shareholder account information, personal financial and other information about shareholders, and passwords and other account access data); (2) investment management information (e.g., portfolio holdings, trading data, and fund accounting information, as well as intellectual property held by a fund complex, such as investment strategies or methodologies and proprietary trading models); and (3) corporate records and other information relating to internal operations (e.g., corporate account information, details about corporate operations, and personal information about officers and employees, including payroll, financial, and medical information). The ongoing operations and financial and reputational health of fund complexes depend on their ability to collect, safeguard, and process such sensitive information quickly and accurately.

Cyber-based threats to the integrity or confidentiality of sensitive information (and of systems for processing such information) take various forms, including misappropriation of information, destruction of information, alteration of information, unauthorized dissemination of information, and interference with the use or processing of information. Although fund complexes appear to have been fortunate to date in having largely avoided significant losses from these types of threats, other businesses (including other financial institutions) have not been so fortunate. Companies are understandably reluctant to provide details on successful cyber-attacks on their systems, and losses sustained by large companies resulting from breach of computer security are typically closely guarded.[7] Yet there are enough recent public reports of significant incidents to underscore that the threats remain very real.[8]

As these recent incidents suggest, computer security intrusions are not solely the work of sophisticated computer "hackers," who are frequently stereotyped as young loners seeking to access seemingly invulnerable systems for the technological challenge (but who may include business competitors or organized crime).[9] Indeed, "insiders" — i.e., current and former employees, including systems administrators and database administrators, as well as outside contractors who have been given full or limited access to an organization's computer systems — arguably pose the greater threat to computer security, both because of the potential scope of their authorized access and because of their knowledge of the potential weaknesses of the organization. While the empirical evidence on whether insiders actually commit the greatest amount of cyber-crime is mixed,[10] it is clear that the potential for harm by insiders may be particularly high.[11] Third parties (e.g., financial intermediaries or business partners) who have been granted limited or even unlimited access to an organization's computer systems may also potentially be perpetrators or may unwittingly — through lax security on their own computer systems — provide platforms through which hackers can access sensitive data of the organization.

Breaches of computer security may have wide-ranging consequences, both direct and indirect, for fund complexes. Computer security breaches may lead to direct financial losses (such as through the misappropriation of proprietary or client assets) or significant indirect financial losses, in the form of costs and expenses associated with detecting, assessing, and repairing affected computer systems, applications, and information and with

restoring customer confidence and trust.[12] Breaches may also result in significant business disruption to affected organizations,[13] and in some cases (as, for example, where breaches result in misappropriation of closely guarded proprietary information) may have an adverse impact on an organization's future business prospects.[14] Computer breaches that lead to unauthorized use or dissemination of sensitive information about shareholders (including the growing problem of identity theft[15]), clients, or employees may also result in reputational damage to an organization,[16] and in some instances may lead to private lawsuits and regulatory actions (e.g., for violations of privacy laws and regulations).[17]

As discussed below, fund complexes use a wide variety of techniques and approaches in designing programs to reduce their risk of losses from computer security risks. Techniques and approaches used by individual complexes necessarily differ as a result of various factors, including a complex's size, the types of computer-based technology used, the scope of its interaction with affiliates and reliance on external service providers, and the complex's overall compliance philosophy and approach to risk management. While there is no single set of best practices appropriate for all fund complexes, the Study suggests that effective computer security risk management efforts are grounded in an appreciation of the following themes:

- Developing a hierarchy of responsibility for computer security issues within a fund complex;
- Identifying and understanding the key computer security risks a complex faces;
- Formulating and implementing a plan to address these risks, in order to prevent breaches in computer security, to detect promptly any incidents that do occur, and to mitigate adverse effects from any such incidents; and
- Retaining knowledgeable, capable, and well-trained employees or consultants to guide the complex's computer security efforts, and increasing and maintaining awareness of computer security risks on the part of management and line-level employees.

In reviewing their efforts to reduce computer security risks, complexes may wish to consider the following general questions, among others.

Appropriate Oversight

How does your complex exercise appropriate oversight over management of computer security risks?

Regulatory authorities have emphasized the importance of a formal hierarchy of management responsibilities for supervision of efforts to limit risks affecting investment management activities.[18] The risks associated with computer security — as potential "franchise risks" that could have severe consequences to the financial health or reputation of a fund complex — merit appropriate oversight by senior management, with appropriate support and assistance from computer security experts and from others in the organization. Mechanisms for providing this oversight may vary from complex to complex. Some complexes, for example, have established a chief technology officer position to oversee the information technology department and overall computer security risk management efforts. Others rely on a committee comprised of management and representatives from departments throughout the organization. Some complexes may directly involve high-level senior management in all new or significant computer security-related issues, such as decisions to permit remote (i.e., off-site) access by employees to e-mail or to various databases. Regardless of the hierarchical structure, many complexes seek broad participation in computer security issues by people throughout the fund organization,

including senior management, and legal and compliance personnel, and representatives from selected business units.

Fund complexes should consider engaging in periodic assessments of their computer security risks and of their programs for managing these risks. At some complexes, such risk assessments may be formal, organization-wide efforts that take place over several months and involve a wide range of personnel (such as the information technology department, legal and compliance personnel, representatives of affected business units, and members of senior management). Other complexes may prefer risk assessments that are less formal, or periodic assessments that are targeted at certain business functions or areas of the organization and include computer security in the context of a broader assessment of operational risks affecting the targeted functions or areas. Some complexes engage the services of outside experts (e.g., audit firms or computer security firms) to assist in such self-assessments.

Strategic and Business Decisions

Does your complex consider computer security in connection with making significant strategic and business decisions?

Fund complexes increasingly view computer security as a vital consideration in overall business planning. Instead of considering the computer security implications of business decisions after the fact and focusing on specific computer-based threats and vulnerabilities as they arise, many fund complexes integrate consideration of computer security concerns directly into the business planning process. Many fund complexes seek advice and counsel from internal or external computer security experts at an early stage in connection with formulating any business initiatives that may implicate computer security concerns. Indeed, some complexes report that information security is a key consideration in determining whether to deploy new software applications or to add functionality to existing applications.

Systems and Procedures

Do you have adequate systems and procedures to prevent and detect unauthorized access to your complex's computer systems?

Most fund complexes have written policies that address many of the procedural aspects relating to computer security. For example, fund complexes frequently implement strict policies on access to computer systems, which encompass both requirements for authenticating a user's identity (e.g., use of passwords) and mechanisms for policing a user's authorization to access particular systems within the complex (e.g., requiring that a security administrator be provided with written permission from a user's supervisor for new or changed access). Such written computer security policies may also address a number of other issues, including confidentiality of data, information retention and destruction, connection of non-approved devices to networks, use of instant messaging and external e-mail accounts, and terms of use for the computer systems. Some complexes report that their policies have become increasingly formal.

In devising systems and procedures to promote information security, fund complexes recognize the critical importance of retaining knowledgeable, capable, and well-trained individuals to guide the complex's computer security efforts. With the frequent emergence of new risks (and variations on old risks), prompt and full-time access to computer security expertise is invaluable. Some complexes, particularly larger complexes, may have separate information technology departments with individuals specializing in various aspects of computer security. Other complexes may rely more heavily on

information technology generalists, with assistance as needed from outside security consultants.

Many computer security experts advise that an organization's *people* — and not its systems or applications — typically present the weakest link in the maintenance of information security.[19] While insider misconduct always remains a risk, carelessness or naïveté on the part of employees poses a greater threat to many complexes. For example, employees often select weak, easily guessed passwords for access to computer systems, or attach notes with their passwords to their computer screens. Employees may also be tricked by outsiders through so-called "social engineering" to divulge passwords or confidential information or may permit strangers access to company premises.[20]

Many fund groups have taken a variety of steps to address the human aspect of computer security risk.[21] Fund complexes frequently include in their employee manuals specific policies and procedures on information security and confidentiality. Some complexes supplement their manuals with periodic bulletins or training about specific means by which information may be obtained through social engineering.[22] For example, some complexes may periodically warn employees not to open suspicious e-mail attachments. In addition, some complexes seek to warn their shareholders against "social engineering" attempts to extract confidential information from the shareholders (through practices such as web spoofing, in which shareholders may receive e-mails directing them to a fraudulent website that appears identical to the complex's website, but instead serves as a conduit to transmit confidential information to the perpetrator).[23]

Fund complexes are also typically sensitive to the potential harm that may result from misconduct by employees, former employees, and contractors or other third parties who have authorized access to parts of a complex's computer systems. Some fund complexes may place particular emphasis on their employment and contracting practices to minimize risk in this area. For example, some fund groups may conduct more extensive background checks on potential employees and contractors than may otherwise be required by law or regulation, particularly with respect to employees, including systems administrators and database administrators, and contractors who are to be provided broad access to computer systems. In addition, some fund complexes may explore the feasibility of obtaining indemnification or other contractual protection from prospective contractors with respect to information security, and to consider the ability of prospective contractors to meet any resulting financial responsibilities they may have to the complex.

Service Providers Affiliates and Third Parties

Do your service providers, affiliates, and other third parties who have been given limited access to your complex's computer systems have adequate protections and procedures to prevent and detect unauthorized access to their own systems?

Third parties (e.g., financial intermediaries, service providers, and business partners) and affiliates who have been given limited access to a fund complex's computer systems may unwittingly — as a result of lax security on their own computer systems — provide platforms through which hackers can access sensitive data of the fund complex. In recognition of this risk, some fund complexes, in appropriate cases, seek assurances as to the effectiveness of the third parties' own computer security efforts. Such assurances may take various forms, including discussions with computer security personnel of the third party, reviews of results of any computer security audits performed on the third party, or requests for an independent review of the third party's computer security program. From time to time, some fund com-

plexes may even seek to arrange for their own computer security personnel to visit the offices of the third party in order to conduct their own on-site review of the third party's computer security protections and procedures. As noted above, some fund complexes may review the feasibility of recovering against third parties, and the ability of such third parties to meet their financial obligations.

Significant Computer Security Incident

Have you considered how your complex will respond to a significant computer security incident?

Because it is impossible, as a practical matter, to prevent all computer security incidents, fund complexes seek to minimize the damage caused by such incidents by developing incident response policies and procedures. With the growth in computer security incidents in recent years, coupled with a heightened concern about the potential consequences of computer security incidents, many fund complexes have devoted more resources to enhancing their computer security incident response capability. Some complexes have, for example, clarified how decisions will be made during an incident, what the chains of command should be, and who should be notified. Some fund complexes have also sought to improve their ability to rapidly assess the threat level of an unfolding incident.

A few fund groups have found it helpful to seek to analyze in advance the probable effects of certain responses to cyber-based incidents. Under some circumstances, for example, fund complexes might conclude that the lost productivity and business disruption resulting from shutting down a computer system will likely outweigh the probable damage from particular types of incidents themselves.

During computer security incidents and especially upon their successful resolution, fund complexes seek to resume normal business operations as quickly as possible. Most fund complexes, particularly after the preparations for the Year 2000 concerns and in the aftermath of the September 11th terrorist attacks, have well-developed backup systems and procedures to prevent loss of systems and data. In recent years, some fund complexes have also developed broader business continuity plans that are aimed not only at recovering from disasters but at increasing their systems' resistance to failure (e.g., through redundant web servers, routers, firewalls, and even entire computer systems in offsite locations).

Fund complexes may also find it useful, in advance, to consider potential sources of recovery for any losses or disruption to the fund complex that may occur as a result of a computer security incident. In this regard, consideration can be given to any contractual protections or recoveries that may potentially be available from service providers, software vendors, and business partners. Fund complexes may also wish to consider the various types of insurance that are available for computer security-related losses.

Elements of an Effective Computer Security Program

Broadly stated, effective computer security programs focus on three key goals: (1) preventing computer security incidents in the first instance, (2) detecting, as quickly as possible, any incidents or attempted incidents that do occur, and (3) mitigating the adverse results of any successful security incident. The Study does not suggest that fund complexes should seek to adopt uniform programs to achieve these goals, given wide variations among fund complexes in size, operational structures, computer systems and applications, and compliance philosophies. However, the Study suggests that effective computer security programs tend to share certain elements and to rely on multiple layers of protection against computer security incidents. The second section of the Study describes these common elements, and discusses questions that fund complexes may wish to consider in structuring their own computer security risk management programs.

Prevention

In seeking to prevent computer security incidents, fund complexes may employ a wide array of defensive techniques. These defensive techniques focus on: (1) blocking avenues for illicit access and use of computer systems, (2) ensuring that access and use is limited to users who are authenticated and authorized to use the computer systems, and (3) devising mechanisms to monitor, audit, and test the defensive techniques implemented by the organization.

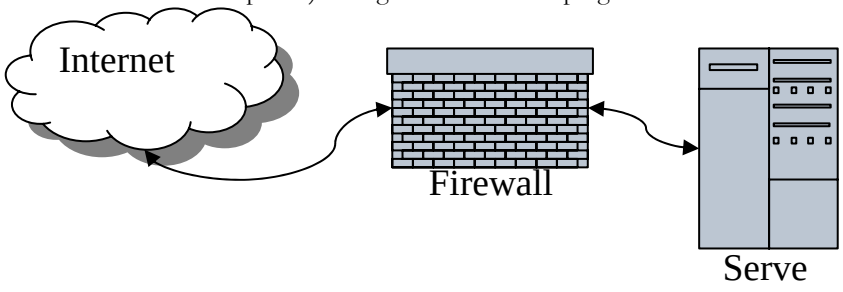
BLOCKING AVENUES FOR ILLICIT ACCESS AND USE OF COMPUTER SYSTEMS

Key Defenses

Fund complexes may use a variety of measures to block illicit access and use of their computer systems. In taking these measures, fund complexes typically recognize that no single defense is foolproof or complete. Types of defenses include "perimeter" protection of computer systems; protection against introduction of viruses and other malicious software; encryption of selected information; and physical security measures. Fund complexes also use a variety of measures to keep their defenses up to date, given the rapid emergence of new vulnerabilities and threats to computer security. In considering these issues, fund complexes may wish to consider the following questions, among others.

- *Use of Electronic "Perimeter" Protections.* To what extent does your complex use firewalls and DMZs to segregate computer systems both from the outside world and from other internal systems? Is more extensive use of such protections warranted?

"Perimeter" protections — in the form of "firewalls" and "DMZs" — form a first line of defense for an organization's computer systems. Computers typically have tens of thousands of entry and exit points (or "ports") through which different programs or services

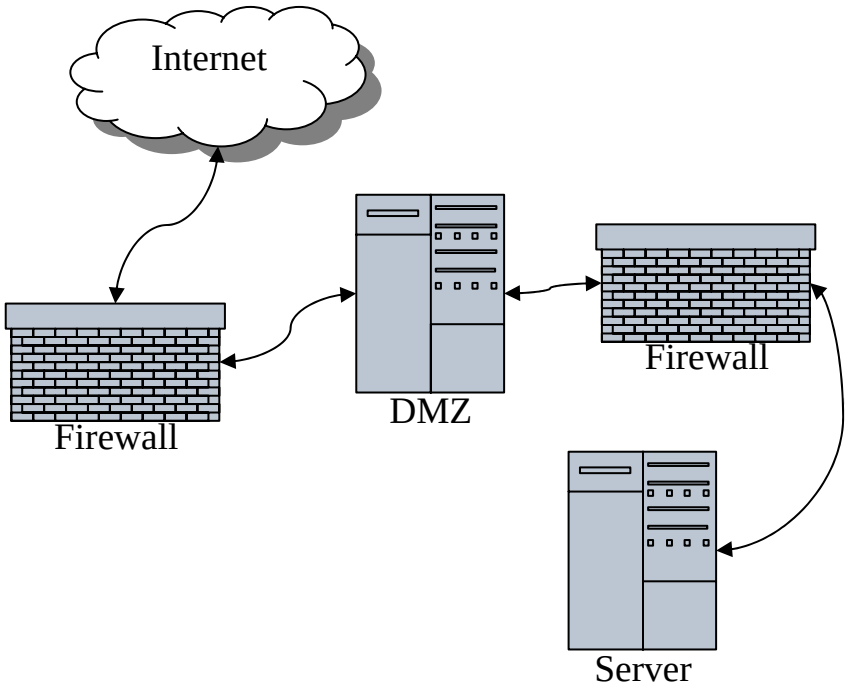


transmit information to and from other computers or networks. "Firewalls" regulate the transmission of inbound and outbound electronic traffic through these ports.[24] In general, firewalls, by default, block all electronic traffic unless such traffic is specifically permitted by pre-established rules and filters. Thus, a firewall may be configured to permit certain types of transmissions (such as e-mail traffic) into and out of an organization's computer systems, but to block other types of transmissions (such as attempts by a rogue software program to access the Internet).

Firewalls are used, generally in the form of firewall servers or routers with firewall protections (and sometimes in the form of software firewalls), by virtually all sophisticated business organizations, including fund complexes.[25] As illustrated in the diagram above, firewalls are generally placed between one computer (e.g., a network server) and outside systems, including the Internet. Many complexes use multiple firewalls to protect different systems from outside intrusions. Although firewalls are most often viewed as barriers against the outside world, they may serve as internal barriers as well. Complexes also frequently use "internal" firewalls to limit the ability of insiders and authorized users to access certain parts of their systems.[26]

Some complexes have redundant firewalls, with automatic switching to backup firewalls in case of failure of the primary firewalls. Many fund groups also seek to enhance the effectiveness of firewalls by closing off all ports that are either unused or that the groups determine should not be used.[27] This limits the number of access points through which a potential intruder is able to penetrate a network.[28] In addition, a few fund complexes are considering the use of personal firewalls, particularly for laptops and home computers that are used by remote users.

Many organizations, including many fund complexes, also employ "DMZs" (demilitarized zones) at certain points in their systems, as an additional level of protection for servers that provide Internet services or for servers that are connected to service providers or affiliates. Ordinarily, as illustrated in the diagram below, a firewall-protected server — the DMZ — is interpositioned between a trusted computer system and external or unknown systems. A DMZ typically contains the minimum amount of data necessary to fulfill a required task, and a successful breach of a DMZ therefore exposes little of the organization's sensitive data to the outside world. Because a hacker must breach an organization's DMZ before attempting to proceed further into trusted systems, the existence of the DMZ increases the likelihood that the hacker's activities will be discovered before the hacker is able to access trusted systems. The existence of a second firewall (i.e., the firewall that is



interpositioned between the DMZ and the organization's trusted network server) also typically assists in making it more difficult for a hacker to reach trusted internal systems (particularly since the second firewall will typically be configured differently from the firewall between the DMZ and the outside world).

Notwithstanding their importance, firewalls and DMZs have certain limitations. They generally do not prevent computer security breaches that are transmitted through permitted channels. Thus, for example, they typically would not prevent an e-mail-borne computer virus from infecting an internal computer system. Moreover, as *perimeter* defenses, firewalls and DMZs do not prevent intrusions, such as intrusions by insiders, that may originate inside the perimeter. Firewalls and DMZs may also have limited effectiveness in preventing intrusions by third-party providers (or other authorized users) of an organization's computer systems, or by hackers who use the systems of authorized third-party providers to access the protected systems.

- *Protection against Introduction of Viruses and Other Malicious Software.* To what extent does your complex employ protections against malicious software? Has your complex considered its position on employee use of instant messaging and external e-mail services? Has your complex considered its position on downloading software from the Internet without prior approval of computer security administrators?

Fund complexes, like virtually all sophisticated business organizations, typically arrange for protections against different types of malicious software that may be introduced into their computer systems.[29] Malicious software may assume numerous forms, including "viruses," "Trojan horses," "worms," "time bombs" or "logic bombs," and "spyware."[30] Malicious software is frequently designed to enter computer systems through legitimate channels, such as via e-mail attachments or through downloads from the Internet of seemingly innocent software. Once active, such software can sometimes propagate rapidly, so as to spread without any further affirmative action on the part of any individual user.

Such software can cause significant damage to computer systems, in the form of disruption or paralysis of normal computer operations, destruction of programs or files, and interference with the integrity of stored information. Recent examples of malicious software attacks include the "Sobig" and "Blaster" worms, which caused widespread disruption to U.S. and international business computer systems in the summer of 2003.[31]

Fund complexes and other organizations commonly rely on various types of "antivirus" software to screen for, and protect against, introduction of malicious software into their systems. As with the use of firewalls and DMZs, the specifics on how such software is employed can significantly affect the level of protection afforded. Complexes may use a variety of antivirus software applications (most commonly, by Symantec or McAfee) at different levels, such as the server level and the workstation level.[32] Some fund complexes report that they scan incoming e-mails with software programs (such as MIMEsweeper) at the firewall gateway, and based on the results of the scan, thereafter review and quarantine or release e-mail attachments.[33] Some fund complexes may also block certain types of files (such as files with a .vbs or .exe extension).

Use of instant messaging and external e-mail accounts (e.g., Yahoo or Hotmail accounts) can increase the risk of malicious software being introduced into an organization's computer systems.[34] Users of such programs do not usually act with malevolent intent, and may even be employing such programs to improve their efficiency (e.g., they do not want to wait for an e-mail attachment to be scanned by MIMEsweeper). However, where

complexes permit use of instant messaging and external e-mail accounts, antivirus software at the workstation level may provide the sole protection against infected e-mail attachments.[35] As a result, the use of instant messaging and external e-mail accounts may permit the entry of transmissions that circumvent the more robust, server-level layers of protection in the system, such as antivirus scanning on the network level and the monitoring of e-mail attachments with MIMEsweeper or equivalent programs.[36] Moreover, because the use of instant messaging and external e-mail accounts is often not systematically tracked by organizations, organizations may be unaware of the scope of transmissions entering their systems through these programs.[37]

Some fund complexes take steps to educate users as to the dangers presented by malicious software, and some may seek to limit the ability of users to circumvent established antivirus protections. Thus, for example, some organizations prohibit downloading of software from the Internet without prior approval of computer security personnel. Similarly, some complexes may prohibit or discourage use by employees of instant messaging or external e-mail accounts.[38] Other fund complexes — particularly those that have not encountered significant issues with malicious software transmitted through instant messaging or external e-mail accounts — may not have developed any formal policies on the use of instant messaging or external e-mails.

Despite the significant protections they provide, antivirus software applications have certain inherent limitations. Thus, for example, such applications may not recognize newly created viruses or worms. The applications are also not designed to detect malicious code (e.g., a "time bomb" or a "logic bomb") introduced by an insider into proprietary software. Moreover, the value of such applications may be reduced if fewer than all computers in a network have been properly updated.

- *Encryption of Selected Information.* To what extent and for what purposes does your complex encrypt data?

Encryption describes the process of encoding data — whether in files or databases or in electronic transmissions — in such a way that it cannot be read without a password. There are a number of encryption algorithms available, which offer varying levels of protection. In general, the strength of an encryption algorithm increases exponentially with the length of the associated password, although the overall strength of an encryption algorithm is also a function of other factors.[39] Encryption algorithms may be "symmetric" or "asymmetric." Symmetric encryption requires an end user to know the exact password with which data was originally encrypted.[40] Although symmetric encryption may be more secure in some respects, it presents a security risk because the password must be conveyed to the end user. By contrast, asymmetric encryption methodologies (including "public key/private key" schemes) allow data to be encrypted with one password and decrypted with another. Such asymmetric methodologies are frequently used for encryption of e-mail transmissions or other types of messages.[41]

The use of encryption by fund complexes appears to vary depending on the type of encryption in question and the intended use of the encryption. Thus, for example, most complexes store passwords to access network systems in encrypted format, which makes it more difficult for intruders (including insiders and authorized users) to access and misuse those passwords. Website transactions also generally have end-to-end security provided by the industry-standard Secure Socket Layer ("SSL") encryption (usually 128-bit). Some complexes use, or are considering the use of, encryption algorithms — such as PGP (Pretty Good Privacy), GnuPG (public-key/private-key encryption schemes) or S/MIME (based on public-key encryption technology

developed by RSA Data Security, Inc.) — to encrypt some e-mail or other messages to affiliates or significant service providers.

Some complexes may also use encryption to secure various system access points. Thus, for example, multi-office complexes may link their offices by encrypted transmissions over virtual private networks ("VPNs"). Fund complexes that provide remote access to employees may also add additional layers of encryption to the SSL encryptions of web transmissions, through use of remote access software (such as Citrix, pcAnywhere, GoToMyPC, or others).

It does not appear that use of encrypted databases (or encrypted fields in databases) is widespread, in part because complexes may view the increased protection afforded by such encryption as outweighed by the loss of performance, convenience, and user functionality. Some complexes also have chosen to limit encryption of data on desktop or laptop computers, in part because of concern that, if an employee is unavailable or forgets the password, there may be no means of recovering the encrypted data on the computer.

Most fund complexes that use encryption do not use proprietary encryption algorithms. Non-proprietary encryption algorithms are typically considered to be more secure than proprietary algorithms, because non-proprietary algorithms are publicly available and thus have been subjected to intense efforts by the cryptographic and "hacker" communities to find and exploit any weaknesses. Proprietary algorithms are typically relatively untested and indeed, may in fact be less secure if the developer has designed a "back door" in the algorithm to permit the vendor access to the encrypted data.[42]

Encryption can provide significant security benefits to an organization, by providing an additional layer of defense to protect the confidentiality of sensitive data if perimeter defenses are compromised. At the same time, encryption may in some cases interfere with prompt access to and recovery of data for legitimate business needs, particularly if passwords are lost or otherwise unavailable. Encryption also cannot readily protect against deletion or destruction of data, or against interference with its use.

- *Physical Security Measures.* What physical security measures are taken by your complex to complement your electronic defenses to breaches of computer security?

Illicit electronic access is not the only type of illicit access to computer systems that may adversely affect an organization. Dangers are also presented by illicit physical access by unauthorized individuals (including unauthorized employees) to servers or other parts of an organization's computer systems. Physical destruction or theft of computer equipment (including easily portable equipment, such as laptop computers or personal digital assistants ("PDAs")) may result not only in expenses associated with loss of the equipment itself, but may in some cases threaten the integrity of the organization's computer systems or information stored therein.[43]

As with other organizations,[44] fund complexes generally are cognizant of the risks posed by illicit physical access, and most take special steps to secure servers and other equipment. Fund groups typically impose some form of control on access to their premises, and may impose special controls for after-hours access. These controls may include keycard entry or the use of badges and dedicated security guards. In addition, some fund complexes impose additional controls on access to specific rooms or buildings where network systems are found. These complexes generally also keep entry logs to track the identities of individuals entering such facilities. (As discussed below, some fund groups also include

physical security in their security assessments and security audits.)

Most fund complexes that provide laptop computers to some or all of their employees have considered whether to take special steps to ensure the physical security of laptops or PDAs (which may have sensitive information stored on them in unencrypted form). Generally, the fund complexes interviewed for the Study have opted not to take extensive measures, in part because the amount of data on laptops tends to be minimal and its sensitivity tends to be low (although there is the possibility that a laptop may contain information to permit remote access by unauthorized users). Moreover, these fund groups tend not to use encryption technology on the laptops, although some groups have considered the use of authentication devices (see Limiting Access and Use to Authenticated and Authorized Users below).

- *Maintenance and Updates of Defenses*. How do you maintain and update your complex's defenses against illicit access to your computer systems? How does your complex learn of potential new vulnerabilities? What are your complex's policies on applying updates and patches to systems and applications?

New vulnerabilities in existing software and hardware are discovered by vendors and the computer security community on a virtually daily basis, and programs that exploit such vulnerabilities may be available with a few days of discovery.[45] Most fund complexes thus believe it is important to take steps to become aware of new vulnerabilities promptly and to remedy serious vulnerabilities — through application of "updates" and "patches" or otherwise — as soon as feasible. Indeed, by some estimates, most security breaches result from exploitation of known, but unremedied, vulnerabilities. Thus, for example, the vulnerabilities exploited by the recent Blaster virus, as well as the Code Red and Nimda "worms," had been well known and widely publicized for at least several weeks before those attacks, and "patches" for those vulnerabilities had been widely available.[46]

One challenge in maintaining defenses is to learn of potential vulnerabilities and remedies for those vulnerabilities in a timely fashion. Given the number and complexity of systems and applications used by fund complexes, it is not surprising that new vulnerabilities may emerge frequently and that there may be numerous patches and updates to those systems and applications available at a given time. Indeed, it may be quite difficult for computer security professionals to keep abreast of all of the available updates and patches.[47]

There are various computer security advisories and alerts that can assist computer security personnel in staying current on known vulnerabilities and remedies. Many of these advisory services are publicly available or are provided at no cost to users of particular systems or applications. Others are fee-based. Software and hardware vendors, such as McAfee, Symantec, Microsoft, and Cisco, typically provide prompt notice of vulnerabilities to their customers.[48] There are also advisories provided by independent third parties, including the Department of Energy's Computer Incident Advisory Capability (CIAC); the CERT Coordination Center (CERT/CC), a part of a federally funded research and development center at Carnegie Mellon University; and the Internet Storm Center, operated by the SANS Institute, a cooperative research and education organization. In addition, the Department of Homeland Security has created the National Cyber Security Division (NCSD) under its Information Analysis and Infrastructure Protection Directorate in order to, among other things, issue cybersecurity alerts and warnings, improve information sharing, and respond to major incidents.[49]

A second challenge in maintaining defenses is to determine when, and how often, to remedy identified vulner-

abilities. A recent study suggests that half of all serious computer security vulnerabilities remained unfixed for at least thirty days (and that less serious flaws may not be fixed for an additional sixty days),[50] allowing sufficient time for hackers and others to develop programs to exploit these vulnerabilities.[51] Yet, as fund complexes have noted, in seeking to achieve greater security by promptly implementing a new update or patch, an organization faces a risk that the update or patch has not been fully debugged. Premature implementation of the update or patch may itself lead to other vulnerabilities. Moreover, on many occasions, updates or patches may themselves undermine computer system stability, which can lead to downtime, productivity losses, and other losses. As a result, most fund complexes seek to test updates and patches before deploying them. Complexes also note the administrative costs of applying patches and updates on too frequent a basis.

Some fund groups seek to update "virus definitions" for antivirus software on at least a weekly basis (with more frequent updates as necessary to address immediate virus threats). Updates and patches for other systems and applications may require different timetables, particularly in light of the difficulties that may be associated with identifying and evaluating available updates and patches for numerous different systems and applications. With respect to known updates and patches, most fund groups seek to apply updates and patches promptly and give the highest priority to updates that address mission-critical vulnerabilities. A few fund complexes treat the existence of vulnerabilities as computer security breaches and respond to them accordingly. Some fund complexes conduct periodic, overall reviews of their systems and applications in order to identify and determine what needs to be upgraded.

Updates and patches are not guarantees against successful computer intrusions. Moreover, the failure to update or patch a single computer on a network may, if such computer is infected, result in the infection of the network.

BLOCKING ILLICIT ACCESS AND PREVENTING ILLICIT USE: SPECIAL ISSUES

In efforts to block illicit access and prevent illicit use of computer systems, special security issues may arise in particular areas, including issues associated with remote access to computer systems by employees and third parties (whether through wired or wireless connections), and with development and use of software applications. In considering these areas in connection with their own operations, fund complexes may wish to consider the following questions, among others:

- *Remote Access to Computer Systems.* If your complex permits remote access to its networks, have you considered the need for any special security protections? How does your complex seek to identify any unauthorized points that may permit remote access to your computer systems?

Remote access to an organization's computer systems — i.e., access by users from locations outside the immediate workplace — is important for many organizations. Remote access by employees (through laptop computers or otherwise) can facilitate productivity, particularly for employees with significant travel obligations, and remote access by business partners and other third parties may be essential to permit an organization to provide appropriate services and otherwise fulfill its business obligations. At the same time, remote access raises special information security concerns. Remote access necessarily "opens" an organization's computer systems to other computers that are outside the immediate physical control of the organization. The security level of these other computers may be unknown by the organization's computer security personnel (or, even if originally

known, may subsequently be modified without their knowledge).

As a result, these "outside" computers may constitute a "weakest link" in an organization's computer security defenses, potentially providing an intruder with an open avenue for accessing the organization's computer systems. Security issues may arise, for example, if a remote user's computer acquires a virus or worm, which is then replicated throughout the complex's computer systems when the remote user establishes a connection. Security issues may also arise if an intruder gains physical or electronic access to a remote user's computer. Because a remote user is normally treated as an insider or authorized user with respect to an organization's computer systems, the organization's firewalls and DMZs are generally configured to permit access to the user and thus would afford limited protection in such cases. Moreover, once an intruder has gained access to one part of an organization's computer systems, it may be easier for the intruder to gain access to other parts of the organization's systems.[52]

Some fund complexes that permit remote access by employees take additional security measures both to authenticate the remote users, and to ensure the security of the connections that are established. With respect to authentication, some fund complexes have established stronger "two-factor" authentication requirements (e.g., use of fobs or tokens, such as RSA SecurID) for remote users. In addition, some complexes have considered limiting the number of employees who are permitted remote access privileges, or defining the scope of an employee's authority to use the organization's systems as a remote user more narrowly than is permitted to that user on-site. With respect to ensuring security of remote connections, some fund complexes may use remote access servers protected by firewalls to handle all remote connection traffic. In addition, some fund groups establish virtual private networks ("VPNs"), which create encrypted tunnels to transmit information over the Internet, to further enhance the security of remote connections.[53] Thus, for example, VPNs are often employed to transmit information between fund complexes and major service providers, such as DST.

As discussed in Auditing and Testing below, many organizations also monitor (or "scan") their own computer systems in an effort to identify any unauthorized access points that could be exploited via remote use.

- *Wireless Access.* Has your complex considered use of wireless LANs, or otherwise permitting wireless access for employees or third parties? If so, what special security steps are being considered?

The security issues presented by remote access in general are particularly acute for organizations that use wireless LANs. Although wireless access to corporate networks can, in theory, be virtually as secure as wired connections, it is generally conceded that there remain security flaws (e.g., weak encryption schemes) associated with most of the wireless technologies currently available.[54] Moreover, some existing vulnerabilities associated with wireless access may be compounded where organizations fail to take those security precautions that are available. For example, many of the protections that are built into wireless access devices (such as password protection, encryption, and the ability not to broadcast the presence of the wireless access point) are frequently disabled by default by the manufacturers of the devices and, in many cases, may not thereafter be enabled by network administrators before the devices are provided to employees or third parties.

Although wireless access to computer systems has been commercially available for several years, it appears that most fund complexes have been wary, to date, about providing such access, primarily out of concern over the

security of such connections. However, some complexes report that they are considering the merits of wireless access, and some are conducting pilot programs of its implementation. Use of virtual private networks and taking full advantage of those security protections that are programmed into many wireless devices can help to reduce — though they are unlikely to eliminate — security concerns.[55]

- *Access and Use by Service Providers and Business Partners.* What steps does your complex take to address the computer security issues arising from the sharing of information with outside service providers and business partners? How does your complex assess the computer security of these entities?

In recent years, fund complexes have increasingly outsourced investment management and related functions, including advisory functions and back-office operations,[56] to service providers and business partners. Fund complexes frequently provide selected service providers and business partners with access and use privileges for various portions of the complexes' own computer systems. As a result, the security of a fund complex's own systems and applications now often depends, in part, on the security of the systems and applications used by service providers and business partners. Because the access provided to service providers and business partners is typically remote access, many of the security issues raised are the same as those discussed above. For example, fund groups may be concerned that a virus infection at the computer systems of a service provider or business partner could spread to the complex's own systems; that an employee of a service provider or business partner may take advantage of the trusted computer connection between the two sets of systems in order to misappropriate information or engage in destructive acts; or that an unrelated third party that has successfully hacked into the service provider's or business partner's systems may thereby be in a position to gain access to the systems of the fund complex, to monitor traffic to those systems, to alter data in transit, or to disseminate confidential information to which it has access.[57]

While recognizing the inherent difficulty of assessing the security of computer networks that are not under their control, fund complexes may take various measures both to assess the level of computer security risks presented by prospective service providers and business partners, and to limit the risks presented by those providers and partners with whom the complexes do business.[58] As an initial matter, in conducting a cost-benefit analysis on whether to outsource a particular function, some complexes include potential computer security concerns as one important factor to be considered. In some cases, particularly in the case of smaller complexes, outsourcing of functions to third parties may result in enhanced information security, particularly if the third parties have specialized expertise in protecting the confidentiality of such information.

Once a decision to outsource is made, many complexes seek to assess the computer security programs of outside service providers and business partners, with the scope of the measures dependent on the sensitivity of information to be shared and on the perceived risks involved. For example, some fund complexes may request and analyze the results of computer security audits of key providers and partners. Perhaps the best-known type of computer security audit is conducted in accordance with the Statement on Auditing Standards No. 70 ("SAS 70"), Service Organizations, developed by the American Institute of Certified Public Accountants. A SAS 70 audit typically focuses on an entity's computer security control activities and processes. In addition, a SAS 70 audit may, but is not required to, include testing of an entity's computer systems.[59] While SAS 70 audits are

likely to provide useful information to a fund complex regarding computer security in place at a service provider or business partner, such audits may have limitations. In this regard, one important limitation is that the scope of a SAS 70 audit is not standardized, but is determined by the subject entity itself, in consultation with its auditor.[60] Although somewhat less prevalent, a few other auditing standards are arguably more objective and more standardized. For example, International Standard 17799 ("ISO 17799"), developed by the International Organization for Standardization and the International Electrotechnical Commission, sets forth a detailed list of controls and security standards for organizations.[61]

In some cases, particularly where the computer security capabilities of a proposed service provider or business partner are relatively unknown, fund complexes may seek to conduct their own on-site reviews or security visits to the organization's computer systems. Under some circumstances, fund complexes may even seek permission from the partner/provider to conduct penetration testing or vulnerability scanning of the partner/provider's computer systems.[62] Moreover, some fund complexes conduct interviews and extensive background research on key providers and business partners and assign risk ratings that are used in considering whether to enter into the contemplated business relationship. In addition to the initial efforts to assess the computer security of service providers and other business partners, some fund complexes also seek ongoing oversight of or periodic reports from key providers and business partners.

Many fund complexes find it helpful to involve their legal personnel in contracting with outside service providers and business partners on issues relating to computer security concerns. Thus, in negotiating contracts with a provider or partner, legal personnel may focus on such issues as the provider/partner's obligations (if any) with respect to maintaining computer systems and to preventing computer security breaches; indemnifying the fund complex for computer security losses traceable to the provider/partner's computer systems;[63] providing the fund complex with notice of changes of status in the provider/partner's users of the fund complex's systems; and maintaining confidentiality of proprietary information or of personal information provided by the complex to the provider/partner. In some cases, a fund complex may seek appropriate assistance from its own analysts to assess whether the provider/partner has adequate financial resources to honor any financial commitments it may make with respect to computer security concerns.

In addition to the foregoing, fund complexes entering into business relationships with service providers and business partners also typically take steps to limit the scope of access of the provider/partner to sensitive systems and data, and to ensure that access is limited to systems and data for which the provider/partner has a legitimate business need. In some cases, fund groups may also set up DMZs between their systems and those of business partners or service providers in order to enhance computer security.

- *Software Security.* What steps are taken by your complex to improve the security of internally developed software applications? Does your complex seek to assess security risks that may be associated with externally developed software?

Software may potentially have vulnerabilities that, if exploited, could permit misuse of the software or misuse of the system on which the software is running.[64] Thus, for example, many software programs have a so-called "buffer overflow" vulnerability in which excess information provided to a program by a user may cause the program to execute unintended and potentially harmful actions.[65] In part, software vulnerabilities may arise

because software developers have traditionally been viewed as focusing primarily on functionality of software, with security as a secondary concern.[66]

Although "standard" software applications may themselves have security vulnerabilities, many observers are also concerned about potential vulnerabilities associated with proprietary software applications (i.e., software either internally developed by a complex or developed specifically for the complex by outside software developers) and with applications and databases that may be developed internally by different business groups within a complex. Most fund complexes use some proprietary software. Such software is common, for example, on portfolio management systems, and in marketing and service areas, where there are often mixes of proprietary and third-party solutions. In addition, much of the software that supports web-based services is often developed or tailored to the individual complex.[67]

Proprietary software applications raise two general types of security concerns. First, because such applications are developed for a limited number of end users, the potential vulnerabilities of the applications may be less well known than those of "standard" applications used by large numbers of businesses. Second, computer security concerns may not always have been adequately considered in the development process for proprietary software, particularly in the case of longstanding "legacy" software that may have been first developed in an era when a fund complex's systems were less accessible to the outside world. With increased exposure of proprietary software to the outside world, any security weaknesses in such software can be at greater risk of being exploited.

In response to these concerns, some fund complexes are taking measures to improve the security of proprietary software and may also take similar measures with respect to "standard" software. Some complexes subject software programs to formal and rigorous security testing by third parties, in addition to an internal security review and a user-acceptance process. In addition, fund complexes that use outside software developers to assist in the development process may seek contractual provisions in their agreements that set security benchmarks and/or add appropriate indemnification provisions.

LIMITING ACCESS AND USE TO AUTHENTICATED AND AUTHORIZED USERS

In addition to blocking avenues for illicit access and use, effective computer security programs also seek to ensure that access and use is limited to users who are authenticated and authorized to use the computer systems. Authentication, broadly stated, describes the process for confirming the identity of a user seeking access to a computer system. By contrast, authorization describes the process for determining the scope of use of a computer system that is permissible for an otherwise authenticated user.

Authentication may involve various factors, depending on what is required of a user in order to establish his or her legitimacy as an individual who is permitted to use particular computer systems. In "one-factor" authentication, identity of a user is tested entirely on the basis of something the user knows which is unique to that user — for example, a password. In "two-factor" authentication, identity of a user is tested not only on the basis of something unique that the user knows, but also on the basis of something unique that the user has — for example, a hardware identification token. In "three-factor" authentication, identity is tested using "biometrics," that is, on the basis of a physical attribute unique to the user — for example, hand topology, fingerprints, or retinal patterns.

Few, if any, users of an organization's computer systems have a legitimate business need to have access to all

facets of all systems. As a result, fund complexes typically develop authorization procedures and systems, such as access control lists administered by dedicated authorization servers, intended to ensure that individual employees and business partners have access only to those systems and applications that permit them to fulfill their business responsibilities, and that other users (such as shareholders) have only the minimum level of access necessary to enable them to obtain the services offered to them by the organization. Thus, for example, many employees (other than employees involved in the shareholder services/transfer agency function) have no legitimate business reason to access personal shareholder information, and as a result, fund complexes do not typically authorize such access for employees.

In considering the scope and nature of procedures for use in authentication and authorization of users, fund complexes may wish to consider the following questions, among others:

- *Authentication Policies.* How does your complex seek to promote strength and confidentiality of passwords? Does your complex require any additional authentication procedures for third party users of your systems or for remote access by employees?

Passwords are currently the most common technique used by organizations, including fund complexes, to authenticate users of their computer systems. Fund complexes commonly have policies designed to promote strength and confidentiality of passwords used by employees for network access, and by third parties for access to information stored on computer systems (such as access by shareholders or brokers to account information). While longer, more complex passwords provide significant additional protections against password "cracking," there is a point at which requiring longer, more complex passwords can be counterproductive, as employees and third party users, in an effort to remember these passwords, may be more likely to write them down in accessible places and thereby compromise their confidentiality. Most fund complexes now appear to require passwords that are at least five, and sometimes as many as seven or eight, characters long. Some complexes impose additional requirements that every password contain both alphabetic and numeric characters, and some may require that passwords that contain "nonsense" characters and/or both upper and lower case letters.

Most fund complexes also actively seek to monitor and enforce their established password requirements. Thus, for example, fund complexes may configure their systems to require default passwords be changed and to prohibit selection by users of passwords that are easily guessed (such as the use of an employee's name or birth date). Many complexes also require that user passwords be changed on periodic basis (e.g., every thirty days, every three months), and some may program their systems to prevent the reuse of passwords previously selected by the user.

Most fund complexes also impose stringent controls on failed attempts to access computer systems. These controls typically involve "locking out" a would-be user after a designated number of failed attempts to enter a correct password (frequently, three to five attempts), with the would-be user thereafter required to contact a designated individual or department to establish his or her identity for purposes of reopening access. Particularly in the case of shareholder access to account information, some complexes are experimenting with use of pre-established electronic means of authenticating a would-be user following a "lock out" on access (e.g., requiring the shareholder to enter unique information previously provided by the shareholder, such as the name of the shareholder's first pet, or the name of the street on which the shareholder lived as a child).

In some fund complexes, different passwords may be required in order for a single user to access different applications or systems. This has the advantage of preventing a potential intruder who has misappropriated an authorized user's password for one system or application from using that password to gain access to all other systems and applications for which the user has authorized access. In some instances, complexes may have deliberately chosen to require different passwords in order to enhance security. In other cases, however, the nature and evolution of the complex's system (e.g., the use of legacy applications or proprietary applications) may effectively mandate the use of different passwords, as it can be difficult or prohibitively expensive and time-consuming to modify the software to permit the use of consistent password requirements. Some complexes report that they are considering the use of a single password approach, and are studying the security implications.

It appears that under the current state of technology, most fund complexes use single-factor authentication for most purposes. However, there is some (although apparently not extensive) use by fund complexes of two-factor authentication procedures, which may involve the use of digital certificates, challenge-response systems, smart cards, or tokens. In particular, some complexes may require two-factor authentication procedures for certain types of access or users, such as for remote access by employees to the complex's computer systems, or for access by outside consultants. There does not appear to be extensive current use of three-factor authentication. Some organizations may be using, or considering use of biometrics, particularly in connection with physical access to facilities housing computer networks. Although the security of such authentication is considered to be quite high, biometrics, like other security measures, is not a complete defense in and of itself.[68]

- *Authorization Policies.* What are your complex's procedures for granting a user access to your networks? What are your procedures for terminating or modifying access if a user changes status?

As with authentication, most fund complexes appear to have developed procedures for authorizing appropriate access for authenticated users. In the case of employees, for example, these procedures frequently require that a senior manager in an individual's department provide the complex's information technology department or security administrator with a written request to permit the employee access to selected systems and applications. Similar procedures may be in place for other categories of users (e.g., consultants, affiliates, service providers). For certain higher levels of access, a fund complex may scrutinize more closely the user's need for such access and may require users to sign limitation-of-use agreements.

These procedures also typically require that changes in a user's status be monitored and their access privileges modified accordingly. If, for example, a user is severing his or her connection with the fund complex, there is usually an exit process during which the user's access rights are terminated. Depending on the circumstances of a user's departure, the termination of access may be expedited or may occur in advance of the departure. Similarly, the procedures often treat other changes in a user's status (e.g., an employee's transfer from one business unit to another) as termination of the previously authorized access and as requiring a new authorization process with a reevaluation of the level of access needed. These procedures are intended to prevent individual users from securing — through inadvertence or neglect on the part of the fund complex — any access that is not currently required by them. In addition, a few fund complexes reevaluate user authorizations on a regular basis and may require some users, particularly

those with a significant level of access, to recertify their need for a given level of access.

As noted above, complexes may pay particular attention to timely termination of access for users — such as terminated employees — who no longer have any legitimate business need to access computer systems or applications. Indeed, disgruntled former employees may present significant computer security risks to organizations.[69] Where third-party institutional users (such as brokers) have access to a fund complex's computer systems, a fund complex may have a limited ability to obtain current information on the employment status of individual authorized users within the third-party organization. In such cases, fund complexes may wish to explore requiring two-factor authentication of authorized users[70] or obtaining appropriate protections through contractual provisions for untimely reporting by the third-party organization of employee changes in status.

AUDITING AND TESTING

In addition to establishing and implementing defensive techniques, effective computer security programs seek to ensure that implemented defenses work as intended and that they address current threats that are known and viewed as serious by an organization. In order to achieve these ends, many organizations routinely engage in both formal and informal audits and self-assessments that address computer security issues. In addition, many computer systems and applications have their own built-in audit functions, which can provide valuable insights into the effectiveness of defensive techniques. Organizations, either directly or with the assistance of outside consultants, may also arrange for testing of their defensive systems, including periodic scans of their systems for vulnerabilities and more extensive "penetration" testing of established defenses.

- *Auditing of Systems, Applications, and Users.* Does your complex conduct computer security audits? If so, what is the scope of the audits and how frequently are they conducted? What standards does your complex use to conduct the audits and evaluate their results?

Many fund complexes conduct periodic audits of their computer security, whether in the form of organization-wide computer security audits, or more narrowly based audits focusing on specific systems, applications, users, or business functions. While some fund complexes prefer to conduct such audits with internal personnel, others seek to engage, on at least a periodic basis, the services of an outside auditor or computer security consultants. These fund complexes cite the benefits of having their computer security programs reviewed by independent third parties, who may frequently be in a position to share information or perspectives gained from their broader experience in studying the computer security programs of organizations with similar structures and facing similar risks. Some fund complexes view the quality of their audits as improved when there is widespread involvement by key departments in their complex, including senior management, legal and compliance personnel, affected business units, and computer security personnel.

Computer security audits conducted by outside auditors are typically conducted in accordance with a set of benchmark standards, such as SAS 70 or ISO 17799. (Even where independent auditors are not involved in review of computer security, many organizations find that SAS 70 or similar control and security standards provide useful guidance for a computer security self-assessment.) In conducting these types of audits, the auditors typically focus on the complex's computer security internal controls and procedures, consider the risks if the control objectives are not achieved, and make recommendations about modifying those controls and procedures to mitigate risks. Auditors may also look at a number of other specific items, such as the availability of

unnecessary computer services (such as FTP or Telnet), the levels of authorization provided to different classes of users, and physical security measures. As discussed in Blocking Illicit Access and Preventing Illicit Use: Special Issues above, the scope of such computer security audits may vary, depending on the standards used and on the agreement reached between a fund complex and the auditor on the appropriate scope of the audit. Once an audit is completed, appropriate individuals (e.g., senior management or audit committee members) may review the results of the audit and the nature of any recommendations contained therein.

In addition, audits performed by regulators, such as the SEC, the New York Stock Exchange, or NASD, Inc., may focus on other compliance issues, but may implicate computer security issues. For example, regulators may examine the policies and procedures that a fund complex has to oversee third-party service providers. Finally, although the SEC has not issued guidelines for assessing network security, other regulators, notably the bank regulators, have issued such guidelines, which may provide a useful benchmark for computer security at financial institutions not subject to the guidelines.[71]

Many systems and applications used by fund complexes also have their own built-in audit functions. For example, a firewall may create log records of the type, volume, and source of traffic that the firewall has permitted or blocked. Moreover, individual systems may also create log records of access attempts by users, as well as the type of computer systems or applications that particular employees have used. In maintaining log records, many fund groups consider a number of issues, including whether the log records should themselves be encrypted, how and where and how long the records are to be kept, and whether any unauthorized changes to the log records can be readily detected. Some complexes may not schedule regular reviews of such log records, but instead may retain the records for subsequent review by a system administrator if an incident is reported. However, as discussed in greater detail below, real-time logging and review of system and application usage may assist a complex in the rapid detection of computer intrusions.

- *Penetration Testing and Vulnerability Scanning.* How does your organization test its computer security defenses and scan for vulnerabilities? Who performs the testing and vulnerability scanning?

In order to ensure that systems are adequately protected, some fund complexes have their computer systems scanned for vulnerabilities. These may include scanning for previously known vulnerabilities that may affect new systems or applications, for newly discovered vulnerabilities, and/or for unauthorized access points (such as unauthorized remote access by employees, e.g., through GoToMyPC or PCAnywhere). Some complexes place considerable importance on scanning their networks for vulnerabilities, and arrange to have their systems scanned by outside security consultants on a regular basis (e.g., quarterly or even monthly) or on demand.[72] A few complexes even use more than one outside computer security consultant in order to obtain different perspectives on their computer systems. Indeed, one computer security expert has stated that vulnerability scanning has the highest impact on computer security with the least effort.[73] Some fund complexes note that vulnerability scanning permits them to allocate their computer security resources more efficiently by helping them evaluate the relative seriousness of different vulnerabilities. As noted above, a few complexes treat vulnerabilities as computer security breaches and respond accordingly.

In addition, many fund complexes periodically test their computer security defenses through attempts to breach various defenses (including firewalls, DMZs, dial-up connections, physical access controls or web servers). In some cases, such "penetration" testing may include

attempts to gather information through social engineering. Penetration tests are often conducted from a number of perspectives. Some fund complexes, for example, conduct penetration testing from the perspective of a hacker or an external authorized user, and a few fund complexes seek to also have penetration testing conducted from the perspective of an employee seeking to damage systems and files to which such employee has access. Some fund complexes conduct their own penetration testing, while others engage the services of outside consultants. Organizations often have strong views (whether for or against) the advisability of using ex-hackers to conduct penetration testing.[74]

Intrusion Detection

As discussed above, fund complexes may employ a wide array of defensive techniques to seek to prevent breaches of computer security. Despite these efforts, attempted breaches of computer security are inevitable, and actual breaches are likely to occur from time to time. The second key goal of an effective computer security program is to detect, in a timely fashion, any breaches or attempted breaches that do occur. Intrusion detection comprises efforts to timely identify not only the fact of an intrusion or intended intrusion, but also its source, scope, and objective.[75] In light of the potential for a very rapid spread of many intrusions (such as self-replicating worms), and the great magnitude of damage that may be inflicted in a short span of time, a focus on intrusion detection can assist both to arrest any incidents before significant damage has occurred, and to safeguard uncompromised systems and data.

- *Intrusion Detection Systems.* How does your complex seek to detect computer intrusions and attempted intrusions? Has your complex considered implementing any intrusion detection products? If so, for what purposes?

Intrusion detection systems may provide an important supplement to an organization's computer security defenses.[76] A number of fund complexes report using, or considering use of, intrusion detection systems, and some fund complexes that currently use intrusion detection systems are considering expanding their use. Although some intrusion detection products resemble firewalls, they differ in certain key respects. In particular, unlike firewalls, intrusion detection products may help detect attacks by insiders or failed attempts to access internal systems and may identify poorly configured firewalls.

Intrusion detection systems are typically set up to examine activity on a computer network to determine either whether certain activity matches the pattern of activity (or "signature") of known attacks, or whether the activity is anomalous for the system in question as measured against a baseline of normal activity for that system. Intrusion detection systems are typically categorized as "network-based" or "host-based." Network-based intrusion detection systems, which typically take the form of separate hardware, monitor electronic traffic traveling over the network, including any traffic traveling through firewalls and DMZs, and seek to identify patterns of use that suggest unusual or suspicious behavior.[77] By contrast, host-based intrusion detection products, typically in the form of software applications residing on the computer or network being monitored, may focus on patterns of attacks, but more typically focus on detecting changes to particular computers, applications, or data files. For example, host-based products may seek to detect intrusions by analyzing audit or log information, or by monitoring the integrity of files[78] to determine whether any unauthorized changes have been made to them.[79]

The placement of an intrusion detection system depends on the nature of intrusion that an organization wishes to

attempt to detect. Thus, if an organization seeks to determine what attacks have passed through a firewall or are being made against a firewall, the system would be appropriately placed, respectively, behind or in front of the firewall. These placements of intrusion detection systems appear to be common among fund complexes using such systems. By contrast, if an organization wishes to detect attacks by insiders, an intrusion detection system would monitor the systems used by those insiders. This placement appears to be relatively less common in the fund industry, although some fund complexes are considering this placement.

In addition to the separate intrusion detection systems described above, there is a broad range of products that have the ability to detect intrusions. Some systems and applications that primarily serve other functions may themselves have intrusion detection capabilities. For example, firewalls may have built-in intrusion detection capabilities and be programmed to alert system administrators if certain conditions are met. Similarly, antivirus software may provide alerts in case of certain types of attacks. Even specific applications may detect unauthorized use of or changes to the applications. Although the intrusion detection capabilities provided by such systems and applications may be less able than stand-alone intrusion detection products to detect network-wide intrusions, they are likely to be better able to detect intrusions of the particular systems and applications themselves.

Some fund complexes monitor their firewalls and DMZs, sometimes as frequently as daily, in an effort to spot patterns that may suggest attempts at illicit access, or vulnerabilities associated with otherwise-permitted electronic traffic. Some complexes also monitor firewalls to determine whether intruders have tampered with their configurations (which could permit previously blocked traffic to pass through the firewall).

Finally, the role of people in an organization in detecting intrusions should not be ignored. Many complexes recognize the value of establishing an incident reporting mechanism for employees to report suspected computer security intrusions. Some complexes, for example, charge every employee with the obligation to report security incidents as well as suspected weaknesses or system malfunctions.

As with any other single element of a computer security program, intrusion detection systems have their limitations. An intrusion detection system may not, for example, recognize a certain pattern of activity as constituting an attack (often referred to as a "false negative"). This may occur for a variety of reasons, including that the usual pattern of activity may be modified slightly to elude detection or that the activity occurs over a sufficiently long period of time that the system does not recognize the activity as a coordinated attack. At the other extreme, an intrusion detection system may erroneously detect attacks (often referred to as "false positives"), creating the risk that a system administrator will ignore all alerts from the system. Because the amount of information logged by an intrusion detection system may be so great as to make impractical any meaningful review of the logs by a system administrator, some companies may use additional software to scan the logs and provide virtually real-time notification of suspected incidents.

In addition, as with firewalls and antivirus software, the effectiveness of intrusion detection systems depends, in part, on their ability to detect the latest form of attack. Fund complexes using intrusion detection systems have recognized that it is therefore important to maintain intrusion detection capabilities by staying up-to-date on vulnerabilities, and assessing and applying available patches or updates as needed.

To a large extent, intrusion detection systems should be viewed as separate computer systems. Thus, fund complexes using intrusion detection products frequently take many of the same steps to protect their intrusion detection capabilities as they do to protect their primary computer systems. For example, because intruders are likely to attempt to disable any intrusion detection capabilities, fund complexes may consider taking measures to protect intrusion detection systems from attack. Indeed, many intrusion detection products have capabilities to detect attempts to compromise the intrusion detection products themselves.

Mitigation

A third goal of an effective program is to mitigate the adverse results of any successful computer security incident, so as to limit damage and disruption from the intrusion, to restore normal business operations as promptly as possible, and to seek any appropriate recovery for losses sustained that may be available from other parties. In developing policies and procedures for mitigating the adverse results of any such intrusion, fund complexes may wish to focus on the following questions, among others.

- *Pre-Incident Planning.* Has your complex considered how it will respond to a computer security incident? Do you have pre-established criteria for determining the threat level? Have you analyzed what the effects would be of shutting down various parts of the computer system?

Fund complexes vary in their approaches to planning for how they will respond to computer security incidents. Some fund complexes may have formal, written documents detailing their plans for responding to a computer security incident, with clear procedures on various topics, such as who will be authorized to make any necessary decisions following an incident and what individuals inside and outside the organization will be notified. Others may engage in less formal consideration of these issues. Similarly, many fund complexes have established response teams to be contacted in the event of an incident, with some complexes using formal incident response team structures and hierarchies, and other complexes approaching staffing needs for incident response more informally. Some complexes seek to ensure that their incident response teams include representatives from a number of different groups in their organizations. Many fund complexes are focusing increased attention on formalizing their incident response structure.

In recent years, particularly after the preparations for the Year 2000 concerns and in the aftermath of the September 11th terrorist attacks, fund complexes have also developed or refined their broader plans for responding to disasters. These plans may provide significant guidance with respect to structuring responses to computer incidents.

Fund groups note the difficulty of seeking to establish, in advance, precise criteria for determining the threat level of a particular type of computer incident and seeking to dictate, in advance, how the organization will respond to each such type. Fund groups point out that the highly uncertain nature of the various potential threats necessarily complicates such an analysis. Some fund groups have established or considered an "escalation process," under which they would, upon the occurrence of an incident, analyze the magnitude, scope, and nature of the incident based on pre-designated criteria, and decide how to react and whom to notify (such as affected business groups, human resources, legal and compliance personnel, affiliates and business partners, Internet service providers, or law enforcement) based on the results of that analysis. Moreover, many fund groups

have sought to evaluate the consequences to their organizations of shutting down various parts of their computer systems in the event of an incident, as well as the relative advantages and disadvantages of promptly shutting down a system versus ongoing monitoring of the penetrated system. Fund groups note that under some circumstances, the damages and disruption resulting from shutting down a system may be more severe than those likely to result from ongoing monitoring.

- *Incident Response.* What steps will be taken immediately upon intrusion detection? Who is to be notified in the event of a network breach? Under what circumstances would your complex issue a public statement regarding a computer security breach?

Regardless of the scope of pre-incident planning, the occurrence of a computer intrusion will likely require a fund complex to address, frequently in a compressed time frame, a number of issues. Upon first detecting an intrusion, a fund complex may have a wide array of options for how to respond. For example, a complex may need to determine whether to shut down, block access to, or quarantine a compromised system or application immediately, or whether to monitor the intrusion in order to determine whether the suspected intrusion is real and to seek to determine the identity and intent of the intruder. As discussed above, either course of action is likely to have different costs and benefits. In making such a decision, a complex would typically consider a number of factors, including the suspected nature or sophistication of the attack, the likely motives of the intruder, and the types of systems and data at risk.

Successful intrusions are likely to require responses from various parts of a fund organization. Thus, for example, in addition to the involvement of computer security personnel, an intrusion may have implications for senior management, legal and compliance personnel, public relations personnel, and even shareholder services representatives. Depending on the nature of the incident, those groups may be contacted or consulted by the computer security personnel. Some fund complexes have established predetermined lists of personnel, which may include personnel at affiliates and service providers, to be notified in the event of different levels of severity of intrusions, and have pre-designated the authority of various personnel to make decisions with respect to responses. Again, the detailed level of disaster recovery plans by fund complexes may address, or at least provide useful guidance, in this regard.

Fund complexes, like business organizations generally, may be understandably reluctant to publicize computer security breaches, in part from concern about adverse publicity or civil liability.[80] Recent legislation in California that requires businesses to notify consumers in the event of certain actual or suspected security breaches may mandate disclosure by fund complexes in some circumstances.[81] It may also be prudent for complexes to consider what obligations, if any, they may have with respect to notifying the Securities and Exchange Commission or other regulators of significant computer security incidents.[82]

Fund complexes, like other business organizations, may be reluctant to share information about security breaches with law enforcement or other third parties, such as information gathering centers (e.g., InfraGard, the National Cyber Security Division ("NCSD"), and Information Sharing and Analysis Centers ("ISACS") for various critical infrastructure sectors).[83] Some fund groups report that they have no predetermined policy regarding cooperation with law enforcement or prosecution of hackers or other intruders. Some law enforcement agencies have strongly encouraged businesses to notify and to cooperate with law enforcement in the event of a significant computer security incident.[84]

Indeed, notification and cooperation has in some cases led to successful prosecution of intruders, and may thereby have prevented or deterred additional incidents.[85]

- *Post-Incident Actions*. Does your complex have a process for analyzing significant computer security breaches? What steps would be taken by your complex to investigate the nature and source of a suspected breach? What steps would be taken to preserve evidence? Does your complex have a policy with respect to prosecution of hackers or other intruders?

In considering what steps should be taken to address computer security incidents, many fund complexes have also considered what actions should be taken post-incident, after the immediate crisis is resolved. In particular, some complexes believe that an in-depth, post-incident analysis of an intrusion can be helpful to ensure that a fund complex does not remain vulnerable to the same type of intrusion and to learn of weaknesses in its overall computer security program and/or in its incident response procedures. Under some circumstances, it may be appropriate to consider a formal incident review, with a report to senior management or the audit committee.

The quality of an incident review may depend in part on the degree to which a fund group has procedures and systems in place that will enable it to uncover and preserve evidence relating to the intrusion. Successful law enforcement efforts may also depend on appropriate preservation of evidence. In some instances, there may be a tension between preservation of evidence and other goals of an organization. Thus, for example, a focus on preservation of evidence may sometimes impair or delay resumption of normal business operations.

- *Data Backup and Disaster Recovery Plans*. What are your complex's policies on data backups? What steps has your complex taken to ensure continuity of operations in the event of large-scale computer security incidents?

Once an organization has completed its immediate effort to arrest and contain the consequences of a computer security intrusion, the organization will typically seek to focus on restoration of any lost or damaged systems or data, or on implementing other back-up plans, in order to resume normal business operations as quickly as possible. A full discussion of data backup and disaster recovery is beyond the scope of this Study. However, as discussed above, much attention has been devoted to these issues in recent years as a result of the planning for the Year 2000 changes, the aftermath of the September 11th terrorist attacks, and, most recently, the large-scale power outage in 2003.[86] In general, fund complexes have developed extensive backup policies and procedures. While complexes have embraced a wide range of policies, most focus on creating regular and automated backups of data and applications and storing those backups in offsite locations. Because backups contain sensitive information, fund complexes should consider what measures it takes to secure those backups.

Some complexes seek more than disaster recovery. In addition, they seek to maintain continuous availability of services, which implies the need to preserve system functionality throughout the course of a computer intrusion. One strategy for doing this used by some fund complexes is to eliminate all single points of failure by having redundant systems. For example, a fund complex may have complete backup systems in an offsite location that is geographically removed from the primary business location, with such systems capable of being activated immediately upon any failure or impairment to primary systems. Fund complexes should also consider whether the backup systems themselves are adequately protected against computer security incidents.

- *Contractual Protections.* To what extent does your complex seek to address computer security issues in engaging the services of third parties?

As discussed above, fund complexes may take various steps to address computer security issues that arise as a result of the complexes' relationships with service providers and other business partners. In particular, fund complexes frequently seek contractual protections in their agreements with those entities to clarify, and in some cases to shift, the burden of losses resulting from computer intrusions.[87]

- *Insurance.* Has your complex evaluated the costs and benefits associated with various types of insurance for computer security incidents?

After analysis of their computer security programs and level of exposure to cyber-related risks, fund complexes may wish to consider whether some form of cyber risk insurance would assist their computer security risk management efforts. Various levels of coverage are available for cybersecurity risks. For example, cyber risk coverage may be available through investment company blanket bonds ("Bonds") and directors and officers/errors and omissions liability insurance policies ("D&O/E&O Policies") commonly secured by fund complexes, although the cyber risk coverage provided under these products tends to be fairly narrow in scope.

Under its Bonds, for example, ICI Mutual offers both (1) "on-line transactions" coverage, which is designed to protect insureds against third-party fraud in redemptions and other transactions in fund shares that are requested via insureds' Internet sites or other secured on-line systems, and (2) "computer security" coverage, which generally is designed to protect against direct loss resulting from hacker attacks or similar unauthorized access to insureds' internal computer systems.[88] Similar coverages are also frequently available under Bonds offered by commercial insurers. Insureds are not generally required to submit to on-site audits or on-site underwriting for these types of coverage, and no additional premium for the coverages is usually charged for insureds who meet qualifying underwriting standards.

Some D&O/E&O Policies, including those of ICI Mutual, may also cover damages that an insured fund complex is required to pay to third parties as a result of the insured's negligence in addressing computer security issues associated with the insured's investment management business. As with the Bond coverages discussed above, insureds are not generally required to submit to on-site audits or on-site underwriting for this type of "errors and omissions" coverage, and no additional premium for the coverages is usually charged for insureds who meet qualifying underwriting standards.

As noted above, it is important to recognize that the cyber-based coverages commonly available under Bonds and D&O/E&O Policies are limited in scope, and are typically subject to various exclusions. Thus, for example, such coverages typically do *not* compensate an insured for many significant losses that can be associated with computer security incidents, such as business interruption expense (e.g., an insured's expense and loss of income after a computer security incident); losses resulting from charges of libel, slander, emotional distress or similar tort-based claims (such as might be brought, for example, by victims of identity theft); 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, including 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.

Broader forms of cyber-insurance have been introduced into the marketplace over the past several years, and are generally issued on a stand-alone basis. These specialty cyber-risk policies are designed to replace and/or supplement the narrower coverages that may be available in other types of underlying insurance policies. These specialty forms are available from various insurers and typically include both "cyber-crime" and "cyber-liability" coverage elements. These specialty policies are designed to cover many of the types of cyber-based losses (discussed above) that are not generally covered under Bonds or D&O/E&O Policies. For these types of specialty policies, prospective insureds may be required to submit to a two-to-three day onsite review by the insurer of their computer systems and applications and their computer security policies and procedures. The costs of reviews are frequently charged to applicants, with the cost credited against the first year premium if the applicant ultimately purchases the broad-based policy. The premiums for such coverage are also significant, and are generally in the range of premiums charged for D&O/E&O Policies generally.

Because the application process typically involves providing outsiders with access to sensitive security information, some organizations have been reluctant to pursue these specialty coverages.[89] Moreover, given the significant expense of such coverages, some organizations have concluded that such insurance would not be cost-effective for them, and that the level of spending on insurance premiums would be better spent on improving computer security.[90] Certainly, as with other aspects of computer security, decisions regarding insurance coverage will vary depending on the needs and concerns of the particular complex. In reviewing their overall computer security programs, fund complexes may wish to carefully review the scope of any insurance coverage they may have for cyber risks, and assess the relative costs and benefits that may be associated with various insurance alternatives.

Endnotes

[1] Fund complexes now typically employ one or more different underlying computer system configurations — typically, mainframe or server computers, local area networks ("LANs"), wide area networks ("WANs"), desktop workstations, or some combination of the foregoing — to support virtually all critical business functions. In addition, most fund complexes also have separate backup computer systems. These backup computer systems mirror all or critical portions of a complex's day-to-day systems, and are designed to permit continuity of critical business functions in the event of disaster or other disruption of primary systems.

Within these computer systems, fund complexes use a wide range of operating systems, such as Unix, Sun Solaris, Microsoft Windows NT or Windows 2000, or Linux, on their mainframes or servers, and may use client versions of those operating systems on employee workstations. These operating systems, in turn, support the use by fund complexes of a broad range of internally or externally developed applications to permit the systems to perform various business functions. Applications may include, for example, (1) proprietary (i.e., internally developed) software for trading and portfolio management, or for client reporting; (2) specialized (and often customized) third-party applications (by Charles River Development, for example) for pre- and post-trade compliance, risk management, customer relationship management, portfolio accounting, web servers, and transfer agency functions; and (3) standard applications (by Microsoft or Oracle, for example) for word processing, e-mail, spreadsheets, presentations, or databases.

Virtually every computer system used by an individual fund complex is connected to one degree or another with one or more other systems. Moreover, fund complexes often permit linkage of parts of their computer systems to separate systems used by affiliates, frequently through use of dedicated lines or virtual private networks ("VPNs") that permit transmission of encrypted data over the Internet. Fund complexes are also outsourcing greater portions of their day-to-day operations (particularly back-office operations and advisory activities), necessitating ongoing transmission and sharing of sensitive information between fund complexes and third-party providers. Many individual fund complexes also now permit fund shareholders and financial intermediaries to access parts of the complex's computer systems, through Internet-based connections or otherwise, in order to allow shareholders and intermediaries access to various types of financial information or to effect account transactions.

[2] A recent study has suggested that up to 60% of fund complexes are outsourcing one or more back-office activities. *See* Suzanne McCoy, *Industry's Compensation, Leadership Norms Shifting*, IGNITES.COM (Aug. 19, 2003), *at* http://www.ignites.com/home/members/article.html?navmode=archive&id=974218061.

[3] Computer security is often analogized to the protection of a castle, with layers of defenses to keep intruders out. Some have noted that this analogy has become increasingly inaccurate as computer systems have become more open and have suggested that a more apt analogy is that of protection of an airport, with numerous people going in and out and with varying levels of security for different areas of the airport. *See SURVEY: DIGITAL SECURITY, When the Door is Always Open*, THE ECONOMIST (Oct. 24, 2002), *at* http://www.economist.com/displaystory.cfm?story_id=1389541.

[4] For example, according to the CERT Coordination Center ("CERT/CC"), a federally funded research and development center that monitors computer security vulnerabilities and tracks incidents involving breaches of computer security, over 82,000 incidents (with each incident, such as an outbreak of a virus, potentially involving thousands of individual computers and networks of computers) were reported in 2002 and over 76,000 incidents were reported in the first six months of 2003. *See CERT/CC Statistics 1988-2003*, CERT/CC, *at* http://www.cert.org/stats/cert_stats.html.

The 2003 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY ("2003 CSI/FBI SURVEY"), *available at* http://www.gocsi.com, a joint survey conducted by the Computer Security Institute ("CSI") and the Federal Bureau of Investigation ("FBI"), reports similar conclusions, based on responses provided by more than 500 organizations (including corporations, government agencies, and financial institutions). According to the 2003 CSI/FBI SURVEY, at 6, 20, over half of all respondents have experienced unauthorized use of their computer systems, with total losses quantified at over $200 million. Over one-third of the reported losses involved theft of proprietary information, and nearly one-third involved denial of service attacks. In its annual survey from 2002, the CSI/FBI reported that Internet connections have become an increasingly frequent point of attack. *See* 2002 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY ("2002 CSI/FBI SURVEY"), at 8.

See also SYMANTEC INTERNET SECURITY THREAT REPORT: ATTACK TRENDS FOR Q3 AND Q4 2002, Report 3, Vol. III, at 16-17 ("SYMANTEC INTERNET SECURITY THREAT REPORT") (Feb. 2003), *at* http://enterprisesecurity.symantec.com/content.cfm?articleID=1964&eid=0, which indicates that 48% of financial services institutions reported a "severe" computer security incident in the last half of 2002, with only power and energy companies having a higher severe incident rate; NATIONAL STRATEGY TO SECURE CYBERSPACE 6 (Feb. 2003), *at* http://www.whitehouse.gov/pcipb ("A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures [including banking, finance, information, and telecommunications].").

[5] This concern has been heightened in recent years by regulatory changes, including the enactment of the Gramm-Leach-Bliley Act and its implementing regulations, such as Regulation S-P. *See* Privacy of Consumer Financial Information (Regulation S-P), Securities Exchange Act Rel. No. 42974 (June 22, 2000).

[6] For example, Microsoft Corporation, Cisco Systems, Inc., the Internal Revenue Service, and America Online, among other well-known organizations, have all reportedly suffered breaches of their computer security systems. *See*, *e.g.*, *Microsoft Not Alone in Suffering Security Breaches*, CNET NEWS.COM (Oct. 27, 2000), *at* http://news.com.com/2100-1001-247734.html; *IRS Security Flaw Crashes Internet Privacy Party*, COMPUTERWORLD (Apr. 12, 2001), *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,59540,00.html; Press Release, *Former Chase Financial Corp. Employees Sentenced for Scheme to Defraud Chase Manhattan Bank and Chase Financial Corporation*, Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice ("CCIPS") (Mar. 21, 2002), *at* http://www.cybercrime.gov/MorchPlea.htm.

[7] *See* 2002 CSI/FBI SURVEY, *supra* note 4, at 20-21 (top reasons cited for non-disclosure of intrusions were fear of negative publicity; concern that competitors would use it to their advantage; a lack of awareness that intrusions could be reported; and a preference for a civil remedy). *See also* NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 4, at 24-25 ("Real or perceived legal obstacles make some organizations hesitant to share information about cyber incidents with the government or with each other. First, some fear that shared data that is confidential, proprietary, or potentially embarrassing could become subject to public examination when shared with the government. Second, concerns about competitive advantage may impede information sharing between companies within an industry. Finally, in some cases, the mechanisms are simply not yet in place to allow efficient sharing of information.").

[8] Examples of recent incidents of computer security breaches include the following:

- *Misappropriation of Information:* In 2000, a citizen of Kazakhstan gained unauthorized access to the computers of Bloomberg L.P. ("Bloomberg"), a multinational financial data company. Posing as Bloomberg customers and employees, the perpetrator accessed numerous personal accounts and obtained personal and business information (including Michael Bloomberg's credit card numbers), as well as information on Bloomberg's internal functions. *See* Press Release, *Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion*, CCIPS (July 1, 2003), *at* http://www.cybercrime.gov/zezevSent.htm.

- *Misappropriation of Information:* In 1999 and 2000, two employees of Chase Financial Corporation exceeded their authorized access of the computer systems of Chase Financial Corporation and Chase Manhattan Bank, and obtained credit card numbers (with an aggregate credit limits of about $580,000) and other account information relating to dozens of customer accounts. They subse-

quently sold the account information to third parties, who, in turn, used the numbers to charge nearly $100,000 in goods and services. *See* Press Release, *Former Chase Financial Corp. Employees Sentenced for Scheme to Defraud Chase Manhattan Bank and Chase Financial Corporation*, CCIPS (Feb. 19, 2002), *at* http://www.cybercrime.gov/williams_turnerSent.htm.

- *Destruction or Alteration of Information:* In 1996, a recently terminated chief computer network program designer at Omega Engineering Corporation activated a "time bomb" (in this case, several lines of malicious code) that permanently deleted all of the company's manufacturing software programs. The organization sustained at least $10 million in lost sales and future contracts. *See* Press Release, *Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced to 41 Months for Unleashing $10 Million Computer "Time Bomb,"* CCIPS (Feb. 26, 2002), *at* http://www.cybercrime.gov/lloydSent.htm.

- *Unauthorized Dissemination of Data:* In February 2003, a hacker compromised the security system of a credit card transaction processor and obtained access to over five million credit card accounts. *See Hacker Accesses 5.6 Million Credit Cards*, CNN.COM (Feb. 18, 2003), *at* http://www.cnn.com/2003/TECH/02/17/creditcard.hack.

- *Interference with Use or Processing of Information:* The spread of the "ILOVEYOU" virus in May 2000 shut down a substantial percentage of business computer systems and disrupted businesses for days. Aggregate losses from the virus, whose origin was ultimately traced to students in the Philippines, have been estimated at nearly $9 billion dollars. James Evans, *Charges Filed Against "Love Bug" Suspect*, NETWORK WORLD FUSION (June 29, 2000), *at* http://www.nwfusion.com/news/2000/0629filed.html.

- *Interference with Web Site:* According to the 2003 CSI/FBI study, 25% of the organizations surveyed suffered unauthorized use or misuse of websites. *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 13. Moreover, Companies with a web site are reported to be 57% more likely to suffer leaks of proprietary information than those without a web presence. "Cyber Threats and the US Economy," CERT/CC (Feb. 2000), *at* http://www.cert.org/congressional_testimony/Cross_testimony_Feb2000.html.

[9] *See, e.g.*, *Studying the Psychology of Virus Writers and Hackers: An Interview with Sarah Gordon*, FRONTLINE (2001), *at* http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/psycho.html (debunking the stereotype that hackers are young, maladjusted loners); *SURVEY: DIGITAL SECURITY, The Weakest Link*, THE ECONOMIST (Oct. 24, 2002), *at* http://www.economist.com/displaystory.cfm?story_id=1389553 (noting that, contrary to the image of the antisocial loner, the most successful hackers may be gregarious experts in social engineering).

[10] *Compare, e.g.*, 2002 CSI/FBI SURVEY, *supra* note 4, at 8 (finding that less than 50% of all reported network attacks come from the inside and noting that Internet connections were more often cited as a frequent point of attack than internal systems); *with SURVEY: DIGITAL SECURITY, The Weakest Link*, *supra* note 9 (citing an estimate from Vista Research that 70% of security breaches involving losses in excess of $100,000 are committed by insiders); SYMANTEC INTERNET SECURITY THREAT REPORT, *supra* note 4, at 26 (noting that over 50% of the computer security incidents to which Symantec responded involved insiders).

[11] *See, e.g.*, *SURVEY: DIGITAL SECURITY, The Weakest Link*, *supra* note 9 (noting that breaches by insiders are "potentially far costlier" than attacks by others).

[12] In 2002, for example, a disgruntled former computer systems administrator at a large broker-dealer allegedly activated a "logic bomb" that he had planted on the company's computer network prior to his resignation. The logic bomb then deleted files on over a thousand computers. The cost of damage assessment and repair reportedly exceeded $3 million. *See Ex-IT worker Charged with Sabotage*, CNET NEWS.COM (Dec. 18, 2002), *at* http://news.com.com/2100-1001-978386.html?tag=fd_top.

[13] In 2001, for example, the spread of the "Code Red" virus shut down large numbers of business computer systems and disrupted many businesses for days. Estimated aggregate business disruption losses exceeded $2 billion. *See, e.g.*, Reuters, *Code Red Costs Reach $2.6 Billion* (Sept. 4, 2001), *available at* http://www.techtv.com/news/securityalert/story/0,24195,3345736,00.html.

[14] In 2000, for example, an employee of Cisco Systems, Inc. exceeded his authorized access to Cisco's computer systems and copied proprietary information about both released products and then-ongoing developmental projects. The individual thereafter submitted his resignation to Cisco and shortly thereafter started working at a potential competitor. *See* Press Release, *San Francisco Man Arrested on Charges of Trade Secrets Theft*, CCIPS (Nov. 21, 2000), *at* http://www.cybercrime.gov/MorchPlea.htm.

[15] Press Release, *FTC Releases Survey of Identity Theft in U.S.: 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers*, Federal Trade Commission (Sept. 3, 2003), *at* http://www.ftc.gov/opa/2003/09/idtheft.htm.

[16] In February 2000, for example, a hacker gained access to Microsoft's source codes for some of its software. As a result, Microsoft mounted a public relations campaign to restore consumer trust. *See Hacker Goes for Heart of Microsoft*, GUARDIAN UNLIMITED (Oct. 28, 2000), *at* http://www.guardian.co.uk/internetnews/story/0,7369,389242,00.html.

[17] Recent federal and state legislation have enhanced the obligations of many organizations, including fund complexes, to safeguard the privacy of their customers. For example, the Financial Modernization Act of 1999 (also known as the "Gramm-Leach-Bliley Act") requires many financial institutions to disclose to their customers their privacy policies and practices with respect to personal information about the customers. Although Regulation S-P, the implementing regulation for the Gramm-Leach-Bliley Act for organizations subject to the SEC's jurisdiction (i.e., broker-dealers, investment advisers, and investment companies), does not impose specific requirements on how an organization must safeguard customer privacy, it does require those organizations to adopt policies and procedures that are "reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer." *See supra* note 5. The Federal Trade Commission ("FTC") has also implemented rules on safeguarding customer privacy, requiring financial institutions to have a written information security plan that describes their safeguards, and specifies, in some detail, what a financial institution must do as part of its plan. In particular, the FTC requires a financial institution to consider all areas of its operation in implementing safeguards, including (1) employee management and training, (2) information systems, and (3) managing system failures. *See* Standards for Safeguarding Customer Information, 67 F.R. 36484 (May 23, 2002).

In addition, California recently adopted the Database Security Breach Act of 2003, which mandates that any business that has suffered, or suspects that it has suffered, a computer security breach of personal information, must notify all of its customers in California of the breach. Similarly, the Department of the Treasury's Office of the Comptroller of the Currency and Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation recently jointly proposed guidelines that would require banks and certain other financial institutions to notify customers in the event of computer security breaches that could lead to identity theft. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 F.R. 47954 (Aug. 12, 2003).

[18] *See, e.g.*, *Back Bay Advisors, L.P.*, Investment Advisers Act Rel. No. 2070 (Oct. 25, 2002); *Quest Capital Strategies, Inc.*, Investment Advisers Act Rel. 1990 (Oct. 15, 2001); *Dawson-Samberg Capital Mgmt., Inc. and Judith A. Mack*, Investment Advisers Act Rel. 1889 (Aug. 3, 2000).

[19] *See, e.g.*, David Gragg, *A Multi-Level Defense Against Social Engineering*, SANS INSTITUTE'S INFORMATION SECURITY READING ROOM (Dec. 2002), *at* http://www.sans.org/rr/papers/51/920.pdf (describing social engineering as "a formidable threat to most secured networks"); *SURVEY: DIGITAL SECURITY, The Weakest Link*, *supra* note 9 (quoting Kevin Mitnick, the well-known hacker, "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain.").

[20] *See*, *e.g.*, *SURVEY: DIGITAL SECURITY, The Weakest Link*, *supra* note 9 (citing a study that two-third of commuters at London's Victoria Station would divulge their password in exchange for a ballpoint pen).

[21] *See* Daintry Duffy, *Test Your Defenses*, DARWIN MAGAZINE (Dec. 2000), *at* http://www.darwinmag.com/read/120100/defenses_content.html; David Gragg, *A Multi-Level Defense Against Social Engineering*, *supra* note 19 (exploiting social engineering to gain access is "never much of an effort," said one security analyst, who added, "We really only do it [i.e., attempt access through social engineering] for the non-believers.").

[22] There are considerable resources available to assist organizations in improving the information security awareness of their employees and other personnel. *See*, *e.g.*, The Human Firewall Council, *at* http://www.humanfirewall.org/default.asp. Symantec Corporation, for example, offers a number of webcasts on a variety computer security issues, including raising the security awareness of employees. *See Beyond Security Awareness — How to Foster Lasting Change in Employee Behavior for a More Secure Workforce*, Webcast, SYMANTEC CORPORATION (Aug. 21, 2003), *at* http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=62; and *Creating a Security Savvy Workforce: How to Build an Employee Security Awareness Program That Works*, Webcast, SYMANTEC CORPORATION (Mar. 20, 2003), *at* http://enterprisesecurity.symantec.com/content/webcastinfo.cfm?webcastid=48.

[23] Press Release, *FBI Says Web "Spoofing" Scams are a Growing Problem*, U.S. Department of Justice, FBI (July 21, 2003), *at* http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm.

[24] Firewalls may exist as a separate hardware appliance or as software (such as Zone Alarm (http://www.zonelabs.com)). Moreover, hardware with other capabilities (including routers) and software with other capabilities may themselves have firewall capabilities. As a rule, firewalls are provided by third-party vendors (such as Cisco (http://www.cisco.com) or Nokia (http://www.nokia.com)). Firewalls themselves have their own operating systems, which are often a standard or specifically modified version of Unix or Linux, or may be an internally developed operating system. For example, Cisco Systems, Inc. has developed its Internetwork Operating System for its routers and other products that have firewall capabilities. In addition, a firewall hardware appliance may itself run specialized firewall software, such as VPN-1/FireWall-1 software from Check Point Software Technologies (http://www.checkpoint.com).

[25] *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 5 (noting that 98% of the respondents to the CSI/FBI SURVEY use some type of firewall).

[26] The importance of separating internal systems with firewalls was illustrated by an incident in early 2003 at a nuclear power plant. After a worm struck the plant, the company discovered that it did not have a firewall separating its corporate computers from those dedicated to the safety of the nuclear reactor. Brendan I. Koerner, *In Computer Security, a Bigger Reason to Squirm*, NEW YORK TIMES (Sept. 7, 2003), *at* http://www.nytimes.com/2003/09/07/technology/07WORM.html.

[27] For example, some fund complexes restrict or block access to services such as the file transfer protocol ("FTP") or Telnet, which may be used to download programs and other files.

[28] *See Achieving Defense-in-Depth with Internal Firewalls*, SANS INSTITUTE'S INFORMATION SECURITY READING ROOM (2001), *at* http://www.sans.org/rr/papers/21/797.pdf.

[29] *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 5 (reporting that 99% of the respondents use some type of antivirus protection).

[30] There are a number of different forms of malicious software, such as "viruses" (which generally infect program and data files, copy themselves without further human intervention, and, among other things, install software, delete files, or send e-mails); "Trojan horses" (which are programs that, like their namesake, seem to be benign, but may be destructive); "worms" (which generally do not infect program and data files, but otherwise are similar to viruses); "time bombs" or "logic bombs" (which execute a series of instructions upon the occurrence of a designated event or after a certain period of time); and "spyware" (which gather information, such as locations of web sites visited, about users and subsequently transmit that information to third parties). *See*, *e.g.*, http://www.matisse.net/files/glossary.html and http://www.netlingo.com/inframes.cfm.

[31] *See* Brian Krebs, *"Good" Worm Fixes Infected Computers*, WASHINGTON POST (Aug. 18, 2003), *at* http://www.washingtonpost.com/ac2/wp-dyn/A9531-2003Aug18?language=printer (noting that the Blaster worm attacked more 500,000 computers); *Sobig is Biggest Virus of All*, BBC NEWS (Aug. 21, 2003), *at* http://news.bbc.co.uk/1/hi/technology/3169573.stm (noting that the Sobig worm was reported at its peak to have infected one out of every 17 e-mails).

[32] Some computer security analysts believe that the antivirus programs on desktop computers will be increasingly unable to respond effectively to more sophisticated and fast-spreading viruses, and that server-level protection against viruses will be necessary. As one chief technology officer stated, "Viruses will soon be too good for desktop computers to stop." *See* Charles Duhigg, *Fight Against Viruses May Move to Servers*, WASHINGTON POST, at E1 (Aug. 28, 2003).

[33] In addition, fund complexes may wish to consider whether their Internet service providers ("ISPs") scan e-mail attachments for viruses before the e-mails even reach the fund complexes. Many ISPs, such as AOL, Microsoft Network, Comcast, and Covad, provide this service. *See* Brian Krebs, *Preventive Medicine for E-Mail*, WASHINGTON POST, at E4 (Aug. 28, 2003).

[34] *See* Stuart Glascock, *Microsoft, FBI, Security Experts Probe Hacking Incident*, TECHWEB NEWS (Oct. 28, 2000), *at* http://www.techweb.com/wire/story/TWB20001027S0009 (suggesting that one likely source of a Trojan horse on Microsoft's internal network was the use of an external e-mail program).

[35] *See* Neal Hindocha, *Threats to Instant Messaging*, SYMANTEC SECURITY RESPONSE WHITE PAPER, at 3 (2003), *at* http://www.symantec.ca/avcenter/reference/threats.to.instant.messaging.pdf (describing instant messaging as "an up and coming threat" and noting the general lack of antivirus applications at the server level that are capable of monitoring instant messaging). In addition, there are an increasing number of malicious software programs (such as W32Choke.Worm) designed to spread through instant messaging. *Id.*

[36] There are currently a few server-level products (such as those by IMLogic Inc. (http://www.imlogic.com), Akonix Systems Inc. (http://www.akonix.com), and FaceTime Communications Inc. (http://www.facetime.com)) that address instant messaging security issues. *See Zone Labs Moves to Secure Instant Messaging*, SECURITY IT WORLD (Aug. 11, 2003), *at* http://security.itworld.com/4357/030811zoneim/page_1.html.

[37] There may also be regulatory implications to the inability to track the use of instant messaging and to retain instant messages. Although the Securities and Exchange Commission ("SEC") is apparently still considering how instant messages should be treated, *see SEC Inspections Will Now Check E-Mail*, IGNITES.COM (Oct. 31, 2003), *at* http://www.ignites.com/home/members/article.html?id=974218958, the SEC does not appear to distinguish between different forms or means of communication. As a result, fund complexes may have the obligation to retain certain instant messages if they otherwise have the obligation to retain the information communicated by instant messaging. *See* Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, Securities Act Rel. No. 7288 (May 9, 1996); Use of Electronic Media for Delivery Purposes, Securities Act Rel. No. 7289 (May 9, 1996). *See also* NASD Notice to Members 03-33 (July 2003) (quasi-governmental agency expressing its view in securities area on retention of instant messaging for records that are similar to those required to be retained by investment advisers and investment companies).

[38] It may be difficult to prevent employees from using external e-mail accounts, particularly in light of the large number of providers of such services. Blocking access to large external e-mail providers may cause employees to use less common providers, which may, in turn, reduce the effectiveness of blocking access to major providers in the event of a computer security incident.

[39] For example, the implementation of the encryption algorithm and the strength of the passwords used affects the practical strength of the algorithm. 56-bit encryption may be cracked relatively easily with readily available processing power, but 128-bit encryption is virtually uncrackable by today's computers. A computer attempting a trillion keys a second would need two quintillion (that is, two million, million, million) years to exhaust all the keys in 128-bit encryption. *See Public Key Cryptography: A Continuation of the Discussion* (July 2001), *at* http://www.avolio.com/columns/pkiq+a.html. Even higher levels of encryption are available, with an accompanying increase in difficulty of decryption. One noted cryptographer, Bruce Schneier, has estimated that, based on the current understanding of quantum mechanics, "the entire energy output of the sun is insufficient to break a 197-bit key" using a brute force attack. *See* Ryan Thomas, *Attacks of PGP: A User's Perspective*, SANS INSTITUTE'S INFORMATION SECURITY READING ROOM (2003), *at* http://www.sans.org/rr/papers/20/1092.pdf.

[40] Examples of different "symmetric" encryption algorithms include AES (the U.S. government standard) and Triple DES, as well as Blowfish and GOST, some of which have never been cracked.

[41] Some common public key/private key encryption techniques include PGP and RSA.

[42] *See* Winn Schwartau, *On Security: To Hell with Proprietary Encryption Algorithms*, NETWORK WORLD FUSION (Aug. 27, 2001), *at* http://www.nwfusion.com/columnists/2001/0827schwartau.html (noting that a public encryption algorithm is preferable to proprietary algorithms).

[43] The potential consequences to the organization can be significant. In December 2002, for example, burglars broke into the offices of TriWest Healthcare Alliance, a health care contractor to the Department of Defense, and stole computer hard drives that contained personal information relating to more than 500,000 people. If the information had been misused, this incident could have resulted in one of the largest identity thefts on record. *Massive Military Medical Info Theft*, CBS NEWS (Dec. 31, 2002), *at* http://www.cbsnews.com/stories/2002/12/31/national/main534819.shtml.

[44] The 2003 CSI/FBI survey indicates that over 90% of respondents also employ physical security measures to enhance their computer security. *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 5.

[45] For example, Cisco recently issued an alert that nearly all of its Internet router models were vulnerable to attack, an alert of particular significance given Cisco's dominant share of the router market. Although Cisco promptly issued a workaround and a software fix, hackers announced within a few days that they had developed programs that could exploit the vulnerability. *See* http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml (released on July 16, 2003).

[46] *See* http://www.cert.org/advisories/CA-2001-26.html (Sept. 18, 2001); http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp (Aug. 15, 2001); *SANS/FBI Top 20 List: The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus*, Version 3.23, SANS INSTITUTE (May 29, 2003), *at* http://www.sans.org/top20.

[47] *See Worm's Spread Slows to a Crawl*, USA TODAY, at 1B (Aug. 14, 2003) (quoting an expert that "[t]he dirty little secret in (technology) today is no organization can keep up with all of the patches available").

[48] Other software vendors and other third parties that provide vulnerability alerts include Sophos (http://www.sophos.com), SystemExperts Corporation (http://www.systemexperts.com), Qualys (http://www.qualys.com), Trend Micro (http://www.trendmicro.com), F-Secure (http://www.f-secure.com), and Vulns.com (http://www.vulns.com).

[49] Additional information is available at the Department of Homeland Security's web site. *See* http://www.dhs.gov.

[50] *See Study: Bad Security Flaws Don't Die*, CNET NEWS.COM (July 30, 2003), *at* http://zdnet.com.com/2100-1105_2-5058058.html. *See also* Dennis Fisher, *Black Hat: Moderate Flaws Threaten Networks*, EWEEK (July 30, 2003), *at* http://www.eweek.com/print_article/0,3668,a=45602,00.asp (noting that "while enterprises are fairly diligent about patching critical software vulnerabilities, they are paying less attention to more moderate flaws and thus leaving their networks exposed to a large variety of vulnerabilities"). For example, a malicious code infected a nuclear power plant's computer systems about six months after the patch to the vulnerability exploited by the code was available. *See supra* note 26.

[51] According to one computer security consultant, for 80% of known vulnerabilities, programs that are able to exploit the vulnerabilities are available within 60 days after the vulnerability is known. *See* http://www.qualys.com/security. Patches may also be reverse-engineered by hackers in order to figure out how to exploit the vulnerabilities. *See, e.g.*, *Microsoft Admits Flaw in Window Software*, WASHINGTON POST (July 17, 2003), *at* http://www.washingtonpost.com/ac2/wp-dyn/A4395-2003Jul17?language=printer (noting that hackers examine Microsoft's patches for clues on how to exploit a vulnerability).

[52] *See* Brendan I. Koerner, *In Computer Security, a Bigger Reason to Squirm*, *supra* note 27 (a worm that entered a company's corporate computers then traveled to other systems).

[53] Other techniques may also be used to enhance the security of remote access, such as the use of remote access software that permits access only to certain applications or the use of web interfaces to certain applications.

[54] *See, e.g.*, *Security of the WEP Algorithm*, *at* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (providing links to papers and presentations on the security vulnerabilities of wireless networks); *Wireless Research*, *at* http://www.cs.umd.edu/~waa/wireless.html (same).

[55] For example, system administrators may change the default passwords, limit the devices permitted to access the wireless access points, enable the wireless encryption scheme provided, and establish more robust authentication protocols.

[56] A recent study suggested that up to 60% of fund complexes are outsourcing one or more back-office activities. Suzanne McCoy, *Industry's Compensation, Leadership Norms Shifting*, IGNITES.COM, *at* http://www.ignites.com/home/members/article.html?navmode=archive&id=974218061 (Aug. 19, 2003).

[57] Such concerns are not unfounded, as illustrated by reported incidents that have affected entities outside the fund industry. In January 2003, for example, a worm entered and disabled a safety monitoring system of a nuclear power plant. The worm first penetrated the computer systems of a contractor, and then entered the nuclear power plant's computer systems over connections established with the contractor's systems. *See* Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, SECURITY FOCUS (Aug. 19, 2003), *at* www.securityfocus.com/printable/news/6767.

[58] *See* BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships, BITS FINANCIAL SERVICES ROUNDTABLE (Oct. 2001), *at* http://www.bitsinfo.org/FrameworkVer32.pdf, for additional resources on managing technology risks that may be raised by the use of service providers.

[59] *See* www.sas70.com/about.htm and linked pages for additional information on SAS 70 audits.

[60] *See* Jonathan G. Gossels, *SAS 70: The Emperor Has No Clothes*, SYSTEMEXPERTS CORPORATION (2001), *at* http://www.systemexperts.com/tutors/sas70.pdf (also noting that SAS 70 audits are performed by auditors who are not necessarily experts in computer security issues).

[61] *See* Jonathan G. Gossels, *ISO 17799: Pay Attention to This One*, SYSTEMEXPERTS CORPORATION (2001), *at* http://www.systemexperts.com/tutors/17799.pdf. In addition, some organizations use the Control Objectives for Information and Related Technology ("CobiT"), developed by Information Systems Audit and Control Association ("ISACA"), for their audits. As with ISO 17799, CobiT sets forth a detailed list of computer security controls and standards.

[62] There are, for example, some programs available (such as AppScan, by Sanctum, Inc. (http://www.sanctuminc.com)) to assist in evaluating the security of systems and applications.

[63] Many indemnification provisions in contracts with service providers seek to limit the amount of indemnification to the fees paid. Fund complexes should consider the sufficiency of such provisions. In any event, the value of an indemnification provision depends, in large part, on the expected solvency of the service provider.

[64] Indeed, it has been estimated that flaws in software design account for 70% of computer security defects. *See SURVEY: DIGITAL SECURITY, Tools of the Trade*, THE ECONOMIST (Oct. 24, 2002), *at* http://www.economist.com/displaystory.cfm?story_id=1389575.

[65] *See*, *e.g.*, *Definition: Buffer Overflow*, *at* http://commons.somewhere.com/buzz/2000/Definition.Buffer.Overfl.html; Michael Legary, *Understanding Technical Vulnerabilities: Buffer Overflow Attacks*, SECCURIS (2003), *at* http://www.seccuris.com/documents/features/Seccuris-Understanding%20Technical%20Vulnerabilities%20-%20Buffer%20Overflow.pdf.

[66] Bill Gates, the chairman of Microsoft, acknowledged the tension between functionality and security, stating, "So now, when we [Microsoft] face a choice between adding features and resolving security issues, we need to choose security." *See Gates Calls for "Trustworthy" Computing*, IDG NEWS SERVICE (Jan. 17, 2002), *at* http://pcworld.shopping.yahoo.com/yahoo/article/0,aid,80183,00.asp.

[67] Some analysts express particular concern about web applications. *See*, *e.g.*, *Is Your Web App Secure? How Do You Know?*, Webcast, SANS INSTITUTE (Sept. 10, 2003), *at* http://www.sans.org/webcasts/show.php?webcastid=90425 (noting that web applications are often "the absolute weakest point of security").

[68] Even the use of fingerprint identification or other biometric technology may not be foolproof. *See*, *e.g.*, SPECIAL REPORT: WORKPLACE SECURITY, *Read My Lips*, THE WALL STREET JOURNAL (Sept. 29, 2003), *at* http://online.wsj.com/article/0,,SB106433084471553900,00.html?mod=sr%2Dworksec%2D2003%5F2; *SURVEY: DIGITAL SECURITY, Biometric Fact and Fiction*, THE ECONOMIST (Oct. 24, 2002), *at* http://www.economist.com/displayStory.cfm?Story_id=1389565; Ann Harrison, *Hackers Claim New Fingerprint Biometric Attack*, SECURITYFOCUS (Aug. 13, 2003), *at* http://www.securityfocus.com/printable/news/6717.

[69] *See*, *e.g.*, *Former Viewsonic Employee Hit with Hacking Charge*, EBN NEWS (Sept. 9, 2003), *at* http://www.ebnonline.com/showArticle.jhtml?articleID=6511957; Press Release, *Former Computer Network Administrator at New Jersey High-Tech Firm Sentenced to 41 Months for Unleashing $10 Million Computer "Time Bomb,"* CCIPS (Feb. 26, 2002), *at* http://www.cybercrime.gov/lloydSent.htm; *Former Intel Employee Admits to Computer Fraud*, CNET NEWS.COM (June 29, 2000), *at* http://news.cnet.com/news/0-1003-200-2174535.html?tag=st.ne.1002.bgif.ni.

[70] The use of two-factor authentication could, for example, make it more difficult for authorized users at a service provider to share their access information with colleagues.

[71] *See Information Security Booklet*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL INFORMATION TECHNOLOGY EXAMINATION HANDBOOK (Dec. 2002), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/information_secruity/information_security.pdf.

[72] SystemExperts Corporation (http://www.systemexperts.com) and Qualys, Inc. (http://www.qualys.com) are examples of security consultants that provide these services.

[73] *See* Dana Graesser, *Cisco Router Hardening Step-by-Step*, SANS INSTITUTE'S INFORMATION SECURITY READING ROOM (July 25, 2001), *at* http://www.sans.org/rr/paper.php?id=794.

[74] *See generally* 2003 CSI/FBI SURVEY, *supra* note 4, at 17 (reporting that over two-thirds of respondents were strongly opposed to the use of ex-hackers for penetration testing). *See also* Deborah Radcliff, *Should You Hire a Hacker?*, SECURITY FOCUS (Apr. 15, 2003), *at* http://www.securityfocus.com/printable/news/3982 (noting the tension between taking advantage of the expertise of ex-hackers and concerns about the degree to which ex-hackers have reformed).

[75] According to the 2003 CSI/FBI survey, 15% of organizations were unaware if their computer systems had suffered unauthorized use or misuse in the previous year. *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 6. Similarly, 22% of organizations reported that they did not know if their websites had suffered unauthorized use or misuse in the previous year. *Id.*, at 13.

[76] The trend among organizations generally appears to be towards greater use of intrusion detection products. According to the 2003 CSI/FBI SURVEY, 73% of the respondents report using some type of intrusion detection system, whereas just 42% reported using such systems in 1999. *See* 2003 CSI/FBI SURVEY, *supra* note 4, at 5.

[77] *See generally* Allison Hrivnak, *Host Based Intrusion Detection: An Overview of Tripwire and Intruder Alert*, SANS INSTITUTE'S INFORMATION SECURITY READING ROOM (Jan. 29, 2002), *at* http://www.sans.org/rr/papers/30/353.pdf.

[78] Programs monitoring file integrity include Tripwire Inc.'s Tripwire (http://www.tripwire.com) and Symantec's Intruder Alert (http://www.symantec.com).

[79] *See Host Based Intrusion Detection: An Overview of Tripwire and Intruder Alert*, *supra* note 77.

[80] See NATIONAL STRATEGY TO SECURE CYBERSPACE, *supra* note 4, at 24-25; *Firms Targeted by Hackers Keep Vulnerabilities Secret*, USA TODAY (Feb. 20, 2003), *at* http://www.usatoday.com/news/opinion/editorials/2003-02-20-our-view_x.htm. There may, however, be benefits to such notification. *See* Esther Gal-Or and Anindya Ghose, *The Economic Consequences of Sharing Security Information* 2, *at* http://www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf (noting that information sharing about security issues may have direct and indirect benefits to companies that share security information and suggesting that such benefits may be greater in competitive industries).

[81] As discussed *supra* note 17, California's Database Security Breach Act of 2003 mandates that, subject to certain exceptions, any business that has suffered, or suspects that it has suffered, a computer security breach of personal information, must notify all of its customers in California of the breach.

[82] Although there do not appear to be any regulations directly requiring an investment company to notify the SEC in the event of a breach, there may be requirements that indirectly have that effect. A fund complex may determine, for example, that a computer security breach is sufficiently significant as to require revision of disclosure documents that are provided to shareholders and that are on file with the SEC.

[83] *See*, *e.g.*, http://www.infragard.net/; http://www.nipc.gov/; Financial Services Information Sharing and Analysis Center, at http://www.fsisac.com.

[84] *See*, *e.g.*, Department of Homeland Security, http://www.dhs.gov/dhspublic/theme_home6.jsp (encouraging reporting of cyber security incidents to the Department).

[85] In the computer intrusion of Bloomberg L.P. by Oleg Zezev, *see supra* note 8, the United States Attorney's office was able to successfully prosecute Mr. Zezev as a result of Bloomberg's cooperation with the FBI, which in turn obtained the cooperation of British and Kazakhstan authorities.

[86] John Schwartz, *Disaster Recovery Plans Get New Scrutiny After Blackout*, NEW YORK TIMES (Aug. 19, 2003), *at* http://www.nytimes.com/2003/08/19/technology/19BACK.html.

[87] As described *supra* note 63 and accompanying text, contractual provisions may be helpful, but have some limitations, in their ability to transfer risk to other parties. Other factors, including the exact language of the indemnification provisions and the solvency and creditworthiness of the service providers and business partners, are also important.

[88] "Computer security" coverage under a bond is designed to protect insureds' internal computer systems against unauthorized access and hacker attacks. Generally, such coverage is "hacker-oriented," as it does not cover attacks committed by or in collusion with insiders or other authorized users, such as third-party service providers.

[89] *See* Debra D'Agostino, *Insuring Security*, *at* http://www.cioinsight.com/article2/0,3959,1215800,00.asp (Aug. 8, 2003).

[90] *See id.*

ICI Mutual | *an uncommon value*

Aligned Interests:
owned by, governed by and operated for mutual funds and their advisers, directors and officers

Mutual Fund Knowledge and Expertise:
tailored, innovative coverage combined with expert claims handling

Stability and Financial Strength in All Markets:
consistent coverage and strong capital

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 to identify and manage risk and defend 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, and independent direction litigation risk, 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.

ICI Mutual Insurance Company, a Risk Retention Group
1401 H Street NW, Suite 1000
Washington, DC 20005

800.643.4246
info@icimutual.com