The Basics of Cyber Insurance

Cyber risks. Cybersecurity breaches are in the news regularly, but those headline-grabbing stories are just the proverbial tip of the iceberg. Cyber attacks are growing rapidly in sophistication and volume—affecting the government, private companies, and financial firms. An FBI internet crime report for 2020 found there were over 19,000 incidents of business email compromise, amounting to adjusted losses of over $1.9 billion. It also noted more than 2,400 ransomware complaints to the FBI Internet Crime Complaint Center. PWC reports that in 2020, "victims of the 11 biggest ransomware attacks have incurred at least $144 million in costs to investigate the attack, rebuild networks and restore backups, pay the ransom and put preventative measures in place to avoid future incidents." An IBM security report says the average total cost of a data breach is $3.86 million. Cybersecurity Venturesestimates that global cybercrime costs will grow by 15% per year over the next five years, reaching $10.5 trillion by 2025.

Cybercrimes create a wide range of business risks, including:

- business email compromise, in which (i) cyber criminals obtain data from emails or (ii) an email that purports to come from an organization is used for nefarious purposes (such as to send a wire payment to a criminal rather than an intended payee);
- ransomware, in which an organization loses access to its own systems and data unless it pays a ransom (and, more recently, simple efforts to deny an organization access to its systems regardless of a willingness to make ransom payments);
- denial of service, in which an organization's clients or staff cannot access the organization's systems because others are clogging its incoming communications lines;
- personal information loss (and possible fines under privacy laws);
- intellectual property loss;
- supply chain risk, where a vendor an organization relies on suffers an attack that impacts the organization (these can be both software [e.g. SolarWinds] or manufacturing [e.g. raw materials not delivered]); and
- income loss to an organization that cannot function due to an incident.

Major cyber actors include organized cyber criminals (who often operate sophisticated networks with their own supply chains), state-sponsored actors, hackers for hire, hacktivists (supporting social causes), third-party vendor attacks (like SolarWinds or other supply chain impacts), and insiders. Also, sometimes employees act inadvertently to give a bad actor access (for example, clicking a link to a malicious website or opening a malicious attachment).

The major risks to a nonprofit organization's investment office include:

- diversion of funds or other valuable assets;
- inability to access key systems, causing a default or inability to take action during a volatile period;

- loss of sensitive employee personal data, as well as data involving an organization's leadership, vendors or prospective vendors, or existing or potential portfolio companies;
- breach of confidentiality provisions in limited partnership agreements and other investment agreements;
- the cost of recovering data and systems; and
- loss of intellectual property, including trade secrets, held by the organization for itself or from third parties.

What can an investment office do to protect itself? First, experts recommend investing in robust, tailored IT controls and training to enhance the security of networks and devices. This includes strong, non-repetitive passwords across accounts, and operating systems that are supported and updated for known issues. Also, an investment office might consider separating its systems from that of its larger endowed organization, especially if that organization interacts across a wider range of users.

Second, the exercise of considering a cyber incident response plan might be helpful. RFG's thoughts on such a plan, which we believe remain relevant even though they were developed a few years ago, can be found here.

Beyond that, cyber insurance may be a prudent choice. RFG turned to Richard May, Strategic Placement Leader of the national cyber practice at EPIC, for more information on the topic. May reports that the majority of financial services organizations his firm deals with, including private equity and family offices, are buying cyber insurance. "However," he adds, "charitable organizations are on the trailing edge."

Unfortunately, over the last year, cyber insurance premiums increased. May reports that the cyber insurance market is split, with smaller organizations seeing increases of 20-50% in their premiums while larger organizations are seeing increases of 30%. He also notes, "Insurers are increasing their scrutiny of systems and processes that can protect against ransomware and are much more ready to decline a risk where they feel there is insufficient risk mitigation in place. Most insurers are requiring completed ransomware supplemental applications prior to providing terms. Missing controls, like multi factor authentication, are increasingly likely to lead to declinations, or subjectivities requiring rectification prior to binding." May adds, "Incumbent insurers (those already providing a cyber policy to the insured) may increase premiums 300% if there is no multi factor authentication." Insurers may also have limits for specific security issues: currently they are sublimiting losses arising from ransomware attacks.

According to May, the following factors have significant potential to impact cyber markets and the availability of cyber coverage:

- growing tension between ransomware and OFAC—creating a moral hazard when paying ransom;
- the evolving privacy regulatory landscape (where affirmative requirements such as the right to be forgotten go well beyond notice requirements);
- gaps and overlapping risks and coverage;
- acceleration of cybercrime in the pandemic; and
- cyberattacks causing physical/bodily injury.

Meanwhile, one columnist notes that increasing attacks both stimulate demand for cyber insurance and create a supply problem by "making insurers warier of providing cover and reinsurers (who provide insurance for insurance providers) less interested in backing cyber liabilities… Ultimately, though, all these drivers boil down to one simple fact: There just isn't enough money in cyber insurance. And it's hard to tell right now if there ever will be."

In response to growing losses in this area, insurers are mandating reviews of the risks: they are seeking information on risk management, employee training, controls and transfer procedures, and implementing restrictions (such as requiring specific security issues to be fixed within a specified time frame, or reducing coverage for ransom as mentioned above). Many insurers have their own ransomware risk supplements that will need to be completed for a new or renewed policy. Thus, obtaining insurance (even on a renewal) can be a time-consuming process.

To address these types of requests from insurers, experts say that the first step to securing coverage is to undergo a cyber risk assessment, including an evaluation of your operational risk (based on reliance on technology); your privacy risk (relating to data on persons you may have in your systems); and security risks. A risk assessment can also include modeling of potential losses. Some organizations that offer frameworks for cybersecurity controls include NIST (National Institute of Standards and Technology) and the Center for Internet Security Top 20 Controls. In addition to risk assessments, service providers also provide vulnerability testing, penetration testing, incident response readiness assessment, and board presentation counseling.

Conducting risk assessments and instituting controls, while necessary and important, does not assure freedom from vulnerabilities. According to cybersecurity practitioner David Kantrowitz at Goodwin Procter LLP, "The recent high-profile supply chain attacks such as SolarWinds and Microsoft Exchange demonstrate that there is a level of baseline risk that cannot be defended against." Kantrowitz added that for customers of SolarWinds or Exchange, there is "no penetration test in the world that would have caught the vulnerability before it happened."

Typical components of a policy. As May explains, there are usually two dimensions to coverage: first-party coverage, which covers losses incurred by the insured party, and third-party coverage, which covers losses of third parties that might seek damages or sue the insured. EPIC provides the following information about these types of coverage.

Typical first-party coverage includes:

- Response for data breach: This covers breach response costs such as forensics, notifications costs, credit monitoring, PR firm services, law firm advice, legal defense, investigation costs, and regulatory fines coverage. However, May notes that most EU countries will not allow insurance to cover GDPR fines as a matter of public policy. Similar concepts might apply in other jurisdictions.
- Business interruption: Typically, this covers lost profits and fixed expenses while the business was interrupted. It pays the difference between profits that would have been generated and what was achieved, and many policies also pay for a forensic accountant to determine the loss. This coverage comes in two types: (1) arising from a security failure (a breach) and (2) arising from an unplanned and unintended system failure (an outage).

There may be a lack of clarity about how these policies apply to an investment organization, as currently the policies are based on a decrease in net income. Net income, however, may not be a defined term. So, in that case, it appears that general accounting principles would apply as to whether there has been a loss of net income. If the trigger is a reduction in net income, would the insured bear the burden of proving that the reduction in net income was caused by an event covered under the policy, as opposed to investment decisions?

- Extortion coverage: According to May, this coverage is in virtually all policies, and it pays ransom demands. In the U.S. this coverage allows the insured to determine whether to pay the ransom (subject to OFAC limitations). The insurers provide coverage for specialist firms to negotiate with the criminal. The insurers also provide advice on how to secure the return of information and an encryption key, and how to avoid the disclosure of protected data. May also notes that a breach coach (for example, a lawyer advising the party being extorted) and a technology forensics firm usually advise on whether the criminal group is on a sanctioned OFAC list. In the past, extortion attempts tended to be either based on paying criminals (i) not to release stolen data or (ii) for decryption. Now, many attacks include both—they steal data and encrypt systems. Both are covered by the extortion coverage. On this topic, aFreshfields podcast noted that there is growing political pressure, at least in the EU, to stop the payment of ransomware demands. This extortion coverage has been a clear driver in carrier losses and is a key factor in the recent pressures in this market, according to Kantrowitz. While payments used to be in the tens or hundreds of thousands of dollars, it is now not uncommon to have multi-million dollar payouts. Kantrowitz says, "It is hard not to wonder if the existence of coverage for extortion itself has not contributed to the rising demands." In fact, recently one insurance company stopped writing these policies in France, which may indicate a future trend. "If insurers stop writing such policies en masse, it could have a tremendous consequence for this black market," says Kantrowitz.
- Extra expense coverage: When business interruption coverage is triggered, a policy would also typically provide for extra expense coverage, such as overtime costs or additional temporary staff or contractors to shorten the interruption, if the extra expense is less than the amount of business interruption loss it is intended to prevent.
- Dependent business interruption coverage: This is triggered if a business the insured depends on (and has a contract with) has a security failure or incident that impedes the insured's business, such that net income decreases. Some policies only provide this coverage for technology providers, while others provide it for "any business you depend on to do business, with whom you have a contract." Dependent business interruption coverage usually also includes system failure coverage triggers, but this is often sublimited by insurers, says May. Again, how this might apply to an investment office will need to be carefully considered.
- Data restoration expenses: This covers the costs of recovering or recreating electronic data caused by a network security breach.

Typical third-party coverage includes:

- Network security/privacy liability: This covers losses arising from failure of network security to prevent the transmission of a malicious code or viruses, or other penetration of the computer system by an unauthorized user (hacker or rogue employee); and failure to

protect non-public personal or corporate information in any format (electronic or hard copy).

- Media liability: Most policies also cover libel, slander, copyright, trademark and other forms of liability arising from publications, speaking, interviews and the like. Like cyber, media is often written by the errors and omissions group at insurers, so these coverages (E&O, cyber and media) are usually packaged together.
- Regulatory proceedings: This covers regulatory proceedings brought by, or on behalf of, a governmental or regulatory authority to enforce privacy laws or regulations. Coverage is available for defense and fines/penalties awarded. This can extend to foreign governments/agencies.

Organizations that provide services to others usually combine their errors and omissions coverage with their cyber insurance. The underwriters are the same, and there is a potential overlap in the E&O coverage and a cyber policy. Because of that, May suggests that it is best to have both insurance policies with the same insurer. This prevents disputes between insurers over which insurer should respond first to an incident that triggers both the E&O and cyber insuring agreements.

Some of the "enhancements" mentioned below are also available on crime policies. Because cyber policies usually have very small sublimits for these coverages, it is often necessary for insureds seeking adequate limits to purchase them on a crime policy as well.

Enhancements to policies. Various policy additions are available. However, they are often sublimited to amounts smaller than the full policy. These include:

- Social engineering: This coverage is typically sublimited to $100,000 to $250,000 and provides protection when a criminal pretends to be someone else and persuades an employee to send funds to an account the criminal controls. This category does not require a computer or any type of hacking. For example, the criminal could use a telephone or the criminal may have used a spoofed email address that tricked the recipient. Most crime insurance policies also include this coverage, often with higher sublimits and better coverage than on a cyber policy.
- Funds transfer fraud coverage: This coverage will apply when someone lacking legitimate authority moves funds electronically using compromised credentials. Unlike social engineering, this is done by the criminal accessing a computer system directly. This coverage is available in cyber and crime policies, but in cyber policies is generally sublimited to $100,000 to $250,000.
- Telecommunications fraud: This is for unauthorized use of insured telecommunications systems resulting in increased telecommunications costs.
- Reputational harm: This covers profit loss due to reputational damage. This usually requires the insured to show that it has lost customers based on a reported incident, and therefore suffered a business income decrease. The focus on loss of customers may make this irrelevant to the typical nonprofit investment office.
- Bricking: This option covers the replacement of equipment, necessitated by a malware attack.
- Utilities coverage: This coverage, generally sublimited to $100,000 to $250,000, pays extra utility costs if someone hijacks the insured's systems—for example, "crypto jacking" to

mine Bitcoin. This would also include telecommunications fraud.

- Invoice manipulation coverage: Invoice manipulation is where a fraudulent invoice is sent from your organization (either altering a legitimate invoice or generating a false invoice) where the entity paying the invoice sends funds to the criminal's account.

Crime policies. Regarding crime insurance for business email compromise, many crime policies require that an insured's loss results "directly" from a triggering act, with no intermediate steps between the hackers' infiltration of the seller's system and the insured's surrender of funds. Thus, Barnes & Thornburg advises that insurers may "contend that this requirement effectively limits coverage to narrow circumstances where a hacker accesses the insured's payment systems and steals money directly from the insured or issues fraudulent instructions directly to a financial institution." Moreover, as some federal appellate courts have ruled in favor of coverage, insurers are revising crime policies "to limit coverage for this kind of loss, either to exclude the loss entirely or add coverage for it back into the policy by endorsement for additional premium."

Best practices. In the same article, Barnes & Thornburg also recommends some best practices for insurance programs, such as:

- Check whether the insurance program includes coverage for social engineering fraud, invoice manipulation, and network security coverage. Is the insurer offering this coverage by endorsement for an additional premium?
- Check the policy limits that apply to those coverages. Binder letters might not disclose a sublimit on certain insuring agreements.
- Consider how excess coverage will apply. If the primary policy has lower coverage limits for some losses, explore whether excess policies will reach these levels to avoid coverage gaps.

The importance of key terms and definitions. Litigation abounds due to disputes on what is covered in these policies. For example, the pandemic caused many employees to work from home on their personal computers—is this part of the covered "computer system" of the employer?

Morgan Lewis advises that "Subtle wording differences can mean the difference between a claim being paid and a claim being denied." For example, May notes, there is a substantial difference between: (i) "computer system owned, operated or leased by the Named Insured" and (ii) "computer system owned, operated or leased by an Insured." Where a policy defines "Named Insured," it usually only incorporates the named entity and its subsidiaries, whereas almost all policies include directors, officers, employees, and independent contractors in the definition of insured.

May points out that these differences may go to the very basis of the policy, because cyber policies are generally designed either to primarily address (i) a data breach (such as ransomware), or (ii) privacy breach. Until GDPR, almost all legislation dealt with data breaches, and the requirements to notify, provide credit monitoring, and the like. GDPR created privacy rights that do not arise from losing data—for example, the right to be forgotten, right of access, right of correction, and right of portability. It also created a private right of actions for these. Not

all cyber policies have coverage that would trigger a claim for damages arising from a breach of these privacy rights.

Evaluating these differences in language is an important part of determining which policy an insured should purchase.

Making a claim. May advises that the first step when an incident occurs is to notify the insurer and provide the information the policy requires, particularly since policies require insured parties engaged in an incident response to use approved law firms, IT/forensic responders, and other vendors. Within a defined period, a sworn "proof of loss" will probably be required if the claim involves loss of money through social engineering fraud, funds transfer fraud, or telecommunications fraud, business income loss, or extra expenses. Some insurers require notification to law enforcement and efforts to recover the funds.