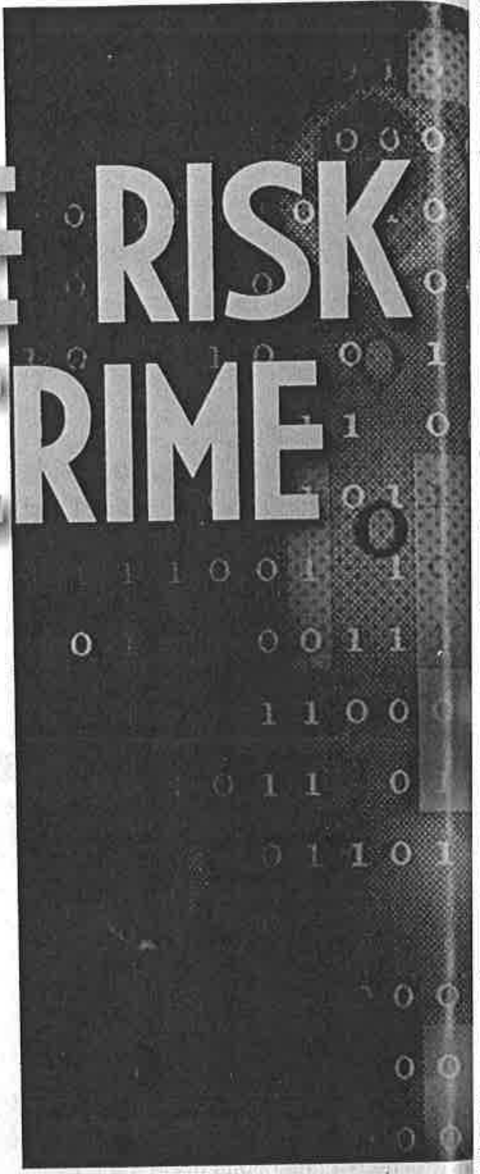
SHIFTING THE RISK OF CYBERCRIME



By Yigal Rechtman

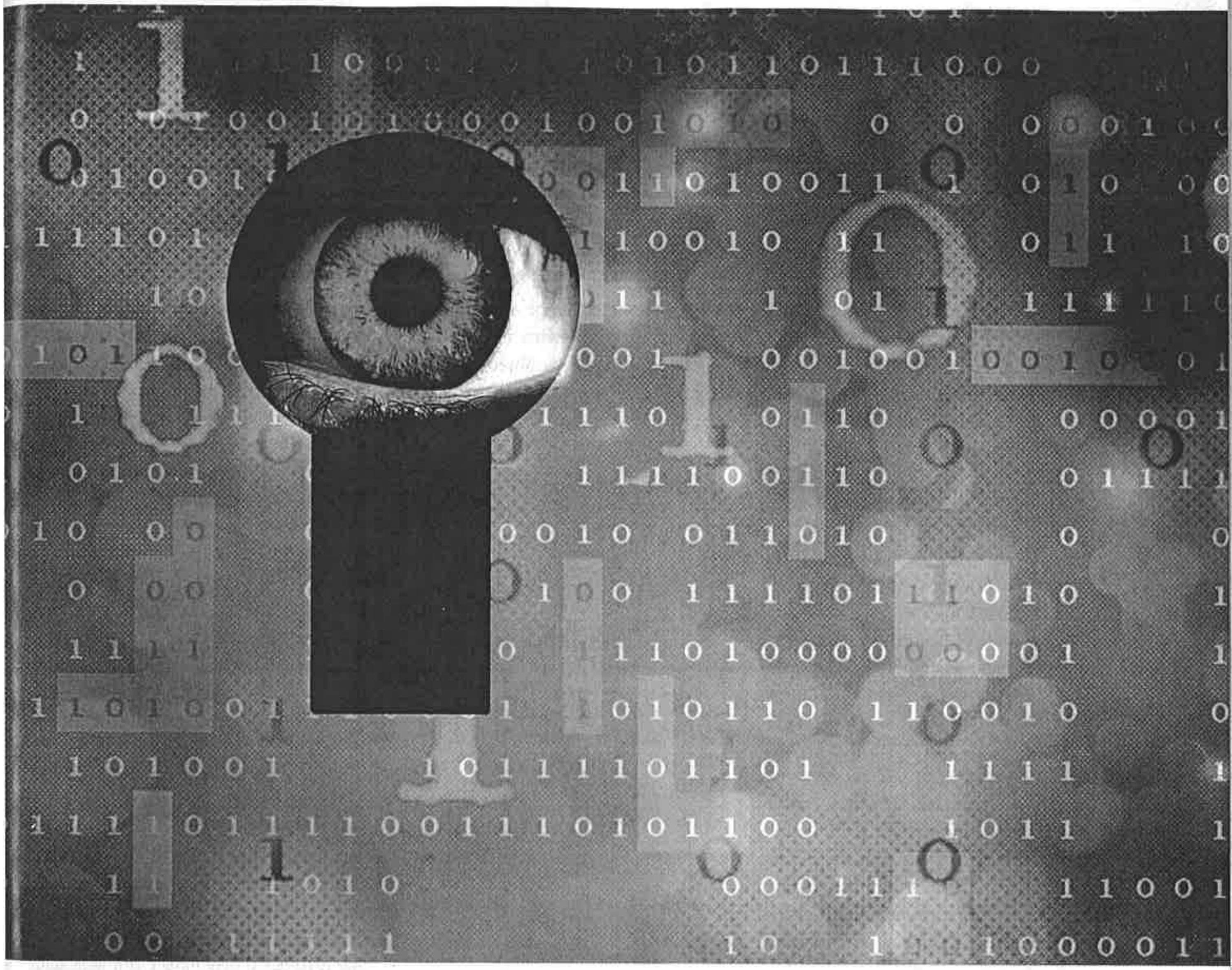
In Brief

The modern digital society has given rise to myriad forms of cybercrime, especially in recent years. To counter this, insurance companies have begun to offer insurance to specifically protect against the threat of digital attacks. The policies available and related premiums and coverage are still developing. The author details the concepts and concerns surrounding cybercrime and recommends steps for businesses considering which insurance to purchase when considering a policy.

The Computer Crime Research Center defines cybercrime as "the commitment of crime using electronic technology means." It can be a theft of assets, a destruction of assets, or a means to convert an asset into a threat (for example, ransomware). Cybercrime can also enable identity theft, social outing (e.g., home addresses of public officials), stalking, and bullying. The Department of Homeland Security has also identified cybersecurity threats to national and commercial interests.

Cybercrime increased rapidly during 2015 and 2016; as a result, information about relevant statistics is somewhat scant. With that in mind, Verizon's 2016 Data Breach Investigations Report estimates that cybercrime related incidents have risen 38% (Bill Laberis, "20 Eye-Opening Cybercrime Statistics," SecurityIntelligence.com, Nov. 14, 2016, https://ibm.co/2riYO0k), and there is no indication that this growth in cybercrime is about to slow. In 2016, the cybersecurity subcommittee of the U.S. House Homeland Security Committee stated that cybersecurity insurance was in its "infancy," that is, with a potential to grow further (Statement of Subcommittee Chairman John Ratcliffe, Mar. 22, 2016, http://bit.ly/2psjvmr). Meanwhile, cybercrime schemes are shutting down large and small organizations with damages to life and property, from the recording office of a small town's police department to large hospitals (Tod Newcombe, "Cybercrime Hits Small Towns," *Governing,* December 2011, http://bit.ly/2psyqNe).

The risk of cybercrime has led to efforts to mitigate exposure. For example, New York State's Department of Financial Services has issued cybersecurity requirements for the businesses that it regulates. Similar actions were seen in increased



enforcement of HIPAA for the Security Rule, as well as increased fines and regulatory oversight for entities that have reported or been found to have security breaches. Businesses are also taking note; a 2016 survey by KPMG reports that 94% of procurement managers consider cybersecurity when evaluating a vendor or supplier *(Small Business Reputation and the Cyber Risk,* http://bit.ly/2qKmESh). This is relevant because many cyberattacks occur when a vendor is electronically interfacing with a company's systems. If the vendor is the weak link in the company's defense system, cyberattacks are more likely. For example, a well-publicized cyberattack against the retailer Target, caused by using the credentials of a contractor, led to damages close to $148 million (Tal Be'ery, "Target Breach Analysis," Feb. 4, 2016, http://bit.ly/2pPHfF6). As of 2016, identified weak links include vendor management, phishing attacks, mobile computing, new software and infrastructure, and cloud-based services. Efforts to mitigate the damage from cyberattacks are likely to continue, with businesses becoming more aware of these weak links and finding better ways to reduce the risk from cybercrime exposure.

One possible response to risk management, albeit less mature and sometimes misunderstood, is obtaining cybercrime insurance. As will be evident from a survey of available policies, only a small share of the insurance market currently provides comprehensive cybercrime policies, with most providers offering only a patchwork of policies with some coverage. The implementation of such coverage, however, is not as straightforward as it appears. It is a multidimensional issue, and this article explores the axes on which the cybercrime insurance implementation rests. First, there is the differentiation between insurers and insured. Second, there is the level of coverage. Third, there is the increased variety of regulatory and even cultural differences that could affect the nature of cybersecurity risk management.

The Insured's Bet

Risk is a theoretical term, but it basically boils down to taking chances and placing bets. Risk can be described in terms of frequency and magnitude. For example, financial auditors who need to assess the risk of material misstatement consider—among other things—the frequency with which an account is being populated with values (e.g., the frequency of sales transactions within a year) and the magnitude of the transactions. In the context of cybersecurity, this might translate to the frequency of weak links in the cybersecurity perimeter and the magnitude of access events via those weak links. For example, if a company's customer list is protected by a well-configured, high-quality firewall, there will be a low frequency of weak links. Coupled with a high-value asset (i.e., the customer list), the company's cybersecurity risk is at an acceptable level. On the other hand, if the company utilizes a low-quality firewall to protect a high-value asset, the higher frequency of weak links makes for an overall high-risk situation.

In general, risk mitigation falls into four categories: accept, share, reduce, or avoid. Insurance shares the risk with the insurer; however, because this is a calculation of chance where the frequency and impact are completely or partially unknown, underwriters—whose responsibility is to assess the risks being assumed—are prone to take a conservative approach and assume that the frequency and impact are high. Doing otherwise could expose the insurance company to a high rate of large claims.

Therefore, insureds and insurers both take bets on what their exposures are. In life insurance underwriting, there is ample experience and industry maturity about human life expectancy. Cyberinsurance, however, is a new field, and insurers and insureds must guess at the level of risk.

Insurance is achieved by executing a contract where coverage and premiums are established. Each party in the contract has its own business objectives. The insurers bet that the insured will never need their services, making the collection of premiums a profitable enterprise; the insureds bet that if coverage is needed, it will be maximized by the nature of the claim. Thus, insurers try to find low-risk policyholders, while insureds try to find high-fidelity insurance companies. Because the two parties are working with incomplete knowledge of the relevant factors, they are both likely to be wrong. For the insured, this could mean inadequate or incomplete coverage; for the insurer, it could mean raising premiums on low-risk clients, driving them away from cyberinsurance altogether.

Cyberinsurance is a new field, and insurers and insureds must guess at the level of risk.

Quality of Coverage

An analysis of cybersecurity coverage presents several issues. The first is the technical definition of the coverage in terms of scope; that is, the value of the coverage versus third-party coverage. Some technical knowledge—not commonly possessed by general agents and underwriters—with respect to the scope of coverage can mean the difference between sufficient and inadequate coverage. For example, some older policies refer to destruction of a hard disk or drive. Most would understand that this is a computer system's main storage area; however, since about 2010, some computers have come equipped with flash memory that is not, technically speaking, a hard drive. Sometimes the terminology difference can be bridged for a specific claim, such as a ransomware attack. Careful analysis of the claim can, however, could still result in a denial of coverage.

Similar inadequacy could be found elsewhere in the policy. For example, when describing hardware infrastructure versus infrastructure as a service (IaaS), one policy excluded software not "owned" by the insured. This terminology proved to be inadequate, because although the rental of infrastructure with IaaS is a leasing arrangement, the risk of loss because of cyberattack still rests with the insured, not with the IaaS operator. Coverage misnomers can also go the other way, where a technology is covered but is not considered by the insurance carrier. For example, copy machines are technically special-purpose computers, and as such have an operating system that could lead to a breach. The same is true for air conditioning systems, fire alarm systems, phone systems, and card-entry readers. If not specifically excluded, these can pose—and have historically posed—an unaccounted-for risk that could lead to additional breaches and cyber-attack. In addition, the policy's definition of "computer system" may be overly narrow. For example, would a company-installed application on an employee-owned mobile device be part of the company's "computer system?" The answer will drive the coverage scope and limits.

In addition, there is the human factor. In its 2016 survey of approximately 2,900 information security professionals, the Information Security Audit and Control Association (ISACA) reported that worldwide, more than half of professionals believe that social engineering (i.e., phishing and other such scams) is the highest cybercrime risk (http://bit.ly/2qTLvPY). In one example, payroll clerks, upon receipt what they thought was a legitimate request, emailed complete copies of Forms W-2 to addresses they thought belonged to their boss or a member of senior management. In reality, the request had been sent by an intruder lurking in the company's network. By the time the company discovered who really received the copies of the payroll records, fake refund requests had been filed on behalf of the unfortunate employees.

This example demonstrates that training and raising awareness are necessary for insureds to avoid an adverse event, as well as for insurance carriers to quantify and price their policies accordingly. For example, if, in the payroll-phishing scheme described above, the e-mail security was not properly enhanced, the insurance carrier might deny parts of the claim because the company's lax security contributed to the breach.

Coverage also includes exclusions and limitations. These are the levers with which the insurance carrier quantifies its own exposure to large claims. When it comes to cybersecurity, however, costs for recovery can be extremely high. When dealing with electronic information systems, the quantities of assets and the ease in which they can be stolen are so large that the costs for recovery may exceed the value of the insured company. For example, for a CPA firm preparing 1,000 personal tax returns and 250 business tax returns, its tax software database contains the identity of approximately 5,000 individuals and entities, as well as approximately 500 bank account numbers. Other databases could contain more information, such as payroll processing, audit and review records, and internal documents about employees. In a 2014 survey, the U.S. Bureau of Justice Statistics (BJS) found that approximately 14% of individual victims experienced an out-of-pocket loss of $1 or more; of these, approximately half lost $99 or less, and 14% lost of $1,000 or more (http://bit.ly/2ql362R). Such figures are not pleasant to contemplate, nor are they practical for a small CPA firm to insure against.

Insurance laws may differ as well; the levels of coverage and definition of a cybersecurity incident vary depending on local law or regulations.

The costs of cybercrime can be overwhelming to an organization of any size. Instead of paying these costs directly, insurance policies focus on the after-the-event costs that could mitigate the losses. It is helpful to note that many insurance carriers offer some level of pre-breach risk management services with the purchase of cyberinsurance coverage. Often, insurance policies will provide for defense costs and other benefits, such as credit monitoring or anti–identity theft tools. Accordingly, companies seeking insurance, and insurance providers themselves, would be well advised to focus not only on the value of the damages—which could grow very quickly beyond anyone's ability to cover—but rather the activities that should be taken once a cybercrime has occurred. To that end, the National Association of Insurance Commissioners has created 12 principles, viewable at http://bit.ly/2qWCLN7.

Questions of Jurisdiction

Obviously, cybercrime can originate beyond the borders of the United States. What may not be considered a protected act in the United States, such as divulging a person's salary, may be a confidential data item in other countries. Furthermore, breach notification protocols differ between nations as well. This is not trivial; if all incidents must be reported to the public, the reputational harm of a company may suffer substantially. Insurance policies thus may need to include remediation for public image and branding in some parts of the world.

Insurance laws may differ as well; the levels of coverage and definition of a cybersecurity incident vary depending on local law or regulations. The determination as to when an incident qualifies as a claim under the policy, and to what extent the coverage applies, would, however, be based on the definition of a claim under the policy itself. Although a full discussion of the legal differences in insurance coverage is beyond the scope of this article, this too should be considered by any U.S.-based organization with business ties, vendors, customers, or property (especially information technology assets) in other countries.

What Should Companies Do?

First, assess the risks. These could vary, and the landscape of cybercrime and cybersecurity is continuously changing. Information technology policies written a year ago may need to be reevaluated, and the scope and level of coverage should also be monitored.

Companies should maintain contact with their information security specialists. Qualified specialists often hold the AICPA's Certified Information Technology Professional (CITP) or ISACA's Certified Information Security Manager (CISM) credentials. These specialists, and not the IT staff, are the right consultants to provide a multidisciplinary understanding of security: people, processes, machines, risk, and financial impact. With the right advisors, a prospective insured should then assess the current level of security. If changes are deemed appropriate and within the organization's own risk tolerance, they should be implemented before cybersecurity policies are evaluated.

Cybercrime insurance questionnaires can be simplistic and sometimes daunting. The daunting ones mean that the carrier is trying to ascertain every possible risk; the simplistic ones mean that the carrier is simply assuming high risk without bothering with details. The objective for the insured should be to find the right policy at the right price. It is also important to note that the insurance application itself is part of the insurance contract; misleading the insurance carrier (intentionally or by error) could constitute a breach of contract.

Small and midsize businesses that wish to have their security assessed may request an assessment based on ISO 27001 or the Control Objectives for Information Technologies (COBIT). Organizations and companies that are Internet service providers may consider undertaking a more sophisticated approach, such as a Service Organization Controls type 2 (SOC-2) attest report with the security criteria included.

The next step is to create a monitoring schedule. In some organizations, monitoring can be added to quarterly checklists; others may find it more practical to monitor the cybercrime insurance policy annually. Organizations that have, for example, a HIPAA checklist could be viewed by insurers as better candidates for a policy because they are likely more proactive.

Third, consider the available policies.

Coverage is often included in different clauses and riders to insurance policies, which can make evaluation and comparison challenging.

Coverage is often included in different clauses and riders to insurance policies, which can make evaluation and comparison challenging. This is a developing insurance market, but some general themes have emerged. Prospective insureds should consider their tolerance for risk, along with an honest assessment of their information technology and cybersecurity. Policies should also be analyzed in terms of the three phases of a cyberattack cycle: attack, resolution, and recovery/monitoring.

After a cybersecurity attack has been remediated, costs could actually rise further from such things as forensic accounting for lost data or records, notification costs to those potentially affected by the attack, identity theft protection, regulatory and civil actions, shareholder suits, legal fees, and damage to brand reputation. There would also likely be a loss of customers and revenues. In addition, victims of publicized cyberattacks become known targets, and cybercriminals may attempt to attack them again. New preventative technology and protocols must be put in place, and regular monitoring should commence. The costs for such normalization and monitoring is also a possible insurable event, which should be specifically mentioned in the insurance contract.

Other policies that could cover cybercrime include errors and omission policies, where claims arising from errors in the company's performance of existing policies are covered; multimedia liability policies, which cover elements of the company's operations such as its website and intangible assets such as customer lists; privacy and confidentiality management insurance, which covers wrongful disclosures of certain regulated data elements such as personal identifying information (PII) or protected health information (PHI); network security and extortion security, which cover assets and costs associated with a misuse of the computer network or ransomware, and can also extend to public relations, ransom payments, and other related costs; and directors' and officers' insurance, which may also include clauses for damages to customers and the entity.

Understanding the underlying business reality of cybercrime is important for business owners and insurers alike. Creating an honest risk evaluation that includes the technical nuances of the underlying technology can help insureds find the right premium and coverage, and guide insurers in providing the same.❑

***Yigal Rechtman, CPA, CFE, CITP, CISM,** is a principal at Grassi & Co., as well as an adjunct professor at the Lubin School of Business, Pace University, New York, N.Y. He is a member of* The CPA Journal *Editorial Board.*